ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Number Theory 104 (2004) 14–61

JOURNAL OF Number Theory

http://www.elsevier.com/locate/jnt

Enumeration of isomorphism classes of extensions of p-adic fields

Xiang-Dong Hou[a,1] and Kevin Keating[b,*]

[a] *Department of Mathematics and Statistics, Wright State University, Dayton, OH 45435, USA*
[b] *Department of Mathematics, University of Florida, Gainesville, FL 32611, USA*

Received 5 September 2001; revised 5 March 2003

Communicated by D. Goss

Abstract

Let Ω be an algebraic closure of $\mathbb{Q}_p$ and let F be a finite extension of $\mathbb{Q}_p$ contained in Ω. Given positive integers f and e, the number of extensions K/F contained in Ω with residue degree f and ramification index e was computed by Krasner. This paper is concerned with the number $\mathfrak{I}(F,f,e)$ of F-isomorphism classes of such extensions. We determine $\mathfrak{I}(F,f,e)$ completely when $p^2 \nmid e$ and get partial results when $p^2 \,||\, e$. When s is large, $\mathfrak{I}(\mathbb{Q}_p,f,e)$ is equal to the number of isomorphism classes of finite commutative chain rings with residue field $\mathbb{F}_{p^f}$, ramification index e, and length s.

MSC: 11S15

Keywords: Class field theory; Enumeration; Isomorphism class; Local field; p-Adic field

1. Introduction

Fix an algebraic closure Ω of $\mathbb{Q}_p$ and let $F/\mathbb{Q}_p$ be a finite extension contained in Ω. Given positive integers f and e, let $\mathscr{E}(F,f,e)$ denote the set of all extensions K/F contained in Ω which have residue degree f and ramification index e. Krasner's formulas in [11–15] allow one to compute the cardinality $\mathfrak{N}(F,f,e)$ of the set

*Corresponding author.
E-mail addresses: xhou@cas.usf.edu (X.-D. Hou), keating@math.ufl.edu (K. Keating).
[1] Research partially supported by NSA Grant MDA 904-02-1-0080.

0022-314X/$ - see front matter
doi:10.1016/S0022-314X(03)00155-0

$\mathscr{E}(F,f,e)$. Suppose $e=p^m e_0$ with $p\nmid e_0$. Krasner's formulas state that

$$\mathfrak{N}(F,f,e)=e\sum_{s=0}^{m}p^s(p^{\varepsilon(s)N}-p^{\varepsilon(s-1)N}), \tag{1.1}$$

where $N=fe[F:\mathbb{Q}_p]$ and

$$\varepsilon(s)=\begin{cases}p^{-1}+p^{-2}+\cdots+p^{-s} & \text{if } s>0,\\ 0 & \text{if } s=0,\\ -\infty & \text{if } s=-1.\end{cases} \tag{1.2}$$

In this paper we consider a related question: What is the number $\mathfrak{I}(F,f,e)$ of F-isomorphism classes of elements in $\mathscr{E}(F,f,e)$? Unfortunately, the formulas for $\mathfrak{I}(F,f,e)$ seem to be much more complicated than those for $\mathfrak{N}(F,f,e)$.

When $p^2\nmid e$, we are able to determine $\mathfrak{I}(F,f,e)$ completely; when $p^2\,||\,e$, we are able to determine $\mathfrak{I}(F,f,e)$ with some additional assumptions on f and e. It is well-known and elementary that $\mathfrak{I}(F,f,e)$ can be computed as a weighted sum over the elements of $\mathscr{E}(F,f,e)$,

$$\mathfrak{I}(F,f,e)=\frac{1}{fe}\sum_{K\in\mathscr{E}(F,e,f)}|\mathrm{Aut}(K/F)|. \tag{1.3}$$

Our method is to use class field theory to determine the groups $\mathrm{Aut}(K/F)$ explicitly.

Besides Krasner's formulas, another motivation for our work is the connections between p-adic fields and finite commutative chain rings. A chain ring is a ring whose ideals form a chain under inclusion. Finite commutative chain rings have applications in finite geometry [10,20] and combinatorics [7,8,16,17]. Since finite commutative chain rings are precisely the nontrivial quotients of rings of integers of p-adic fields, classifying isomorphism classes of finite extensions of $\mathbb{Q}_p$ is essentially equivalent to classifying isomorphism classes of finite commutative chain rings. In particular, in Section 2 we will show that $\mathfrak{I}(\mathbb{Q}_p,f,e)$ is equal to the number of isomorphism classes of finite commutative chain rings with residue field $\mathbb{F}_{p^f}$, ramification index e, and length s, for all sufficiently large s.

The paper is organized as follows. Section 2 is a summary of the connections between p-adic fields and finite commutative chain rings. Section 3 contains some preparatory results about p-adic fields. In particular, we determine the $\mathbb{F}_p[\langle\gamma\rangle]$-module structure of $K^\times/(K^\times)^p$, where K is a finite extension of $\mathbb{Q}_p$ and γ is a $\mathbb{Q}_p$-automorphism of K. In Section 4 we consider the problem of computing $\mathfrak{I}(F,f,e)$ when $p\nmid e$. Besides calculating $\mathfrak{I}(F,f,e)$, we also collect some facts about tamely ramified extensions of F which will be used later in the paper. In Section 5 we determine $\mathfrak{I}(F,f,e)$ in the case $p\,||\,e$. Sections 6–10 are devoted to calculating $\mathfrak{I}(F,f,e)$ in the case $p^2\,||\,e$, with some additional restrictions on f and e. In Section 6 we outline the computational plan and determine the structures of

certain Galois groups. The key ingredients in the formula for $\mathfrak{I}(F,f,e)$ are computed in Sections 7–9, and the final formula is assembled in Section 10.

For $K\subset\Omega$ a finite extension of $\mathbb{Q}_p$, we let $n_K=[K:\mathbb{Q}_p]$ be the degree of $K/\mathbb{Q}_p$. We denote the ring of integers of K by $\mathcal{O}_K$, the maximal ideal of $\mathcal{O}_K$ by $\mathcal{M}_K$, and the residue field of K by $\bar{K}=\mathcal{O}_K/\mathcal{M}_K$. Any generator π_K for $\mathcal{M}_K$ is called a uniformizer for K. We let v_K denote the valuation on K normalized so that $v_K(\pi_K)=1$ for any uniformizer π_K. Then v_K extends uniquely to a valuation on Ω which takes values in $\mathbb{Q}$, and is also denoted v_K. In particular, we let $v_p=v_{\mathbb{Q}_p}$ denote the valuation on Ω which satisfies $v_p(p)=1$. Let L be a finite extension of K. Then the residue degree $[\bar{L}:\bar{K}]$ of L/K is denoted $f(L/K)$, and the ramification index $v_L(\pi_K)$ of L/K is denoted $e(L/K)$. Finally, let $\{\zeta_a : a\geqslant 1\}$ be a compatible system of primitive roots of unity in Ω, with ζ_a a primitive ath root of unity and $\zeta_{ab}^b=\zeta_a$ for every $a,b\geqslant 1$.

2. p-adic fields and finite commutative chain rings

In addition to the description in terms of p-adic fields given in Section 1, there is another more explicit construction of finite commutative chain rings based on Galois rings; we refer the reader to [18] for more details. Choose a prime p, positive integers n,f, and a monic polynomial $\Phi\in(\mathbb{Z}/p^n\mathbb{Z})[X]$ of degree f whose image in $(\mathbb{Z}/p\mathbb{Z})[X]$ is irreducible. The ring $\mathrm{GR}(p^n,f)=(\mathbb{Z}/p^n\mathbb{Z})[X]/(\Phi)$ is called the Galois ring of characteristic p^n and rank f; it is determined up to isomorphism by p, n, and f. Every finite commutative chain ring is isomorphic to a ring of the form $R[X]/(\Psi,p^{n-1}X^t)$, where $R=\mathrm{GR}(p^n,f)$ is a Galois ring, $\Psi\in R[X]$ is an Eisenstein polynomial of degree e, and

$$\begin{aligned} &t=e && \text{if } n=1,\\ &1\leqslant t\leqslant e && \text{if } n\geqslant 2. \end{aligned} \tag{2.1}$$

The integers p,n,f,e,t are called the invariants of the finite commutative chain ring [1].

The following proposition summarizes the connections between finite commutative chain rings and p-adic fields.

Proposition 2.1. *Let $K/\mathbb{Q}_p$ be a finite extension, with residue degree f and ramification index e, and let $k/\mathbb{Q}_p$ be the maximal unramified subextension of $K/\mathbb{Q}_p$. Let s,t,n be positive integers such that $s=(n-1)e+t$, with $1\leqslant t\leqslant e$, and let $\tilde{\Psi}$ denote the image of $\Psi\in\mathcal{O}_k[X]$ in $(\mathcal{O}_k/p^n\mathcal{O}_k)[X]$. Then we have the following.*

(i) *Let $a\in\mathcal{O}_k$ be such that $\bar{k}=(\mathbb{Z}/p\mathbb{Z})[\bar{a}]$, where $\bar{a}$ is the image of a in $\bar{k}$, and let $\Phi\in\mathbb{Z}_p[X]$ be the minimal polynomial of a over $\mathbb{Q}_p$. Then the image $\tilde{\Phi}$ of Φ in $(\mathbb{Z}/p^n\mathbb{Z})[X]$ is monic of degree f and the image $\bar{\Phi}$ of $\tilde{\Phi}$ in $(\mathbb{Z}/p\mathbb{Z})[X]$ is irreducible. Therefore*

$$\mathcal{O}_k/p^n\mathcal{O}_k\cong(\mathbb{Z}/p^n\mathbb{Z})[X]/(\tilde{\Phi})\cong\mathrm{GR}(p^n,f). \tag{2.2}$$

(ii) *The minimal polynomial of π_K over k is an Eisenstein polynomial $\Psi \in \mathcal{O}_k[X]$ of degree e such that*

$$\mathcal{O}_K/\pi_K^s\mathcal{O}_K \cong (\mathcal{O}_k/p^n\mathcal{O}_k)[X]/(\tilde{\Psi}, p^{n-1}X^t) \cong \mathrm{GR}(p^n,f)[X]/(\tilde{\Psi}, p^{n-1}X^t), \quad (2.3)$$

where $\tilde{\Psi} \in (\mathcal{O}_k/p^n\mathcal{O}_k)[X] \cong \mathrm{GR}(p^n,f)[X]$ is an Eisenstein polynomial over $\mathrm{GR}(p^n,f)$. Thus $\mathcal{O}_K/\pi_K^s\mathcal{O}_K$ is a finite commutative chain ring with invariants

$$\begin{array}{ll} (p,1,f,t,t) & \text{if } n=1, \\ (p,n,f,e,t) & \text{if } n>1. \end{array} \quad (2.4)$$

Moreover, every finite commutative chain ring is isomorphic to $\mathcal{O}_K/\pi_K^s\mathcal{O}_K$ for some finite extension $K/\mathbb{Q}_p$ and some $s \geqslant 1$.

(iii) *Assume $s > \left(\frac{p}{p-1} + v_p(e)\right)e$ and let $L/\mathbb{Q}_p$ be another finite extension. Then $\mathcal{O}_K/\pi_K^s\mathcal{O}_K \cong \mathcal{O}_L/\pi_L^s\mathcal{O}_L$ if and only if $K \cong L$.*

Proof. Statements (i) and (ii) are well-known.

(iii) We want to prove that if $\mathcal{O}_K/\pi_K^s\mathcal{O}_K \cong \mathcal{O}_L/\pi_L^s\mathcal{O}_L$ with $s > \left(\frac{p}{p-1} + v_p(e)\right)e$ then $K \cong L$. Note that $s > \left(\frac{p}{p-1} + v_p(e)\right)e$ implies $n > 1$. Thus the residue degree and ramification index of $L/\mathbb{Q}_p$ are determined by $\mathcal{O}_L/\pi_L^s\mathcal{O}_L \cong \mathcal{O}_K/\pi_K^s\mathcal{O}_K$, and so $L/\mathbb{Q}_p$ also has residue degree f and ramification index e. We may assume that K and L are both contained in the algebraic closure Ω of $\mathbb{Q}_p$. Then $K/\mathbb{Q}_p$ and $L/\mathbb{Q}_p$ have the same maximal unramified subextension $k/\mathbb{Q}_p$, and K/k and L/k are both totally ramified extensions of degree e. We may assume that $e > 1$. Let $\Psi \in \mathcal{O}_k[X]$ be the minimal polynomial of π_K over k. The assumption $\mathcal{O}_K/\pi_K^s\mathcal{O}_K \cong \mathcal{O}_L/\pi_L^s\mathcal{O}_L$ implies that

$$(\mathcal{O}_k/p^n\mathcal{O}_k)[X]/(\tilde{\Psi}, p^{n-1}X^{t-1}) \cong \mathcal{O}_L/\pi_L^s\mathcal{O}_L. \quad (2.5)$$

By Lemma XVII.8 in [18] there exists $\boldsymbol{\sigma} \in \mathrm{Aut}(\mathcal{O}_k/p^n\mathcal{O}_k)$ such that $\boldsymbol{\sigma}\tilde{\Psi}$ has a root $\beta \in \mathcal{O}_L/\pi_L^s\mathcal{O}_L$. Let $b \in \mathcal{O}_L$ be a lifting of β. Since $\boldsymbol{\sigma}\tilde{\Psi} \in (\mathcal{O}_k/p^n\mathcal{O}_k)[X]$ is an Eisenstein polynomial of degree $e < s$, it follows that $v_L(b) = 1$. Since $k/\mathbb{Q}_p$ is unramified, the natural homomorphism $\mathrm{Gal}(k/\mathbb{Q}_p) \to \mathrm{Aut}(\mathcal{O}_k/p^n\mathcal{O}_k)$ is an isomorphism. Let $\boldsymbol{\Sigma}$ be the element of $\mathrm{Gal}(k/\mathbb{Q}_p)$ whose image in $\mathrm{Aut}(\mathcal{O}_k/p^n\mathcal{O}_k)$ is $\boldsymbol{\sigma}$. Then $\boldsymbol{\sigma}\tilde{\Psi} = \widetilde{\boldsymbol{\Sigma}\Psi}$, so the image of $(\boldsymbol{\Sigma}\Psi)(b)$ in $\mathcal{O}_L/\pi_L^s\mathcal{O}_L$ is $(\widetilde{\boldsymbol{\Sigma}\Psi})(\beta) = (\boldsymbol{\sigma}\tilde{\Psi})(\beta) = 0$. Therefore $v_L((\boldsymbol{\Sigma}\Psi)(b)) \geqslant s$.

Let $r_1, r_2, \ldots, r_e \in \Omega$ be the roots of $\boldsymbol{\Sigma}\Psi$; then $(\boldsymbol{\Sigma}\Psi)(X) = \prod_{i=1}^e (X - r_i)$. We may order the r_i so that $m = v_p(b - r_1)$ is as large as possible. Then for $2 \leqslant i \leqslant e$ we have $v_p(b - r_i) \geqslant \min\{m, v_p(r_1 - r_i)\}$. If $m > v_p(r_1 - r_i)$ then $v_p(b - r_i) = v_p(r_1 - r_i)$, while if $m \leqslant v_p(r_1 - r_i)$ then by the maximality of m we get $v_p(b - r_i) \leqslant v_p(r_1 - r_i)$. It follows that for $2 \leqslant i \leqslant e$ we have $v_p(b - r_i) \leqslant v_p(r_1 - r_i)$. Since $(\boldsymbol{\Sigma}\Psi)(b) = (b - r_1)$

$(b-r_2)\dots(b-r_e)$, this implies

$$\frac{s}{e}\leqslant v_p((\Sigma\Psi)(b))\leqslant m+\sum_{i=2}^{e} v_p(r_1-r_i)=m+v_p(\delta_{k(r_1)/k}), \tag{2.6}$$

where $\delta_{k(r_1)/k}=(\Sigma\Psi)'(r_1)$ is the different of the extension $k(r_1)/k$. By Remark 1 of [19, p. 58] we have $v_p(\delta_{K/k})\leqslant 1-e^{-1}+v_p(e)$. Since we are assuming $s>\left(\frac{p}{p-1}+v_p(e)\right)e$, this implies $m>\frac{1}{p-1}+e^{-1}$. Using Lemma 2.2 below we get $\frac{1}{p-1}+e^{-1}\geqslant v_p(r_1-r_i)$, and hence $m>v_p(r_1-r_i)$ for all $2\leqslant i\leqslant e$. It follows by Krasner's lemma (see [12, p. 224]) that $k(b)\supset k(r_1)$. Since $[k(b):k]=[k(r_1):k]=e$, we get $L=k(b)=k(r_1)\cong K$. □

Lemma 2.2. *Let k be a finite extension of $\mathbb{Q}_p$, let $\Psi\in k[X]$ be an Eisenstein polynomial of degree e, and let $r_1,r_2,\dots,r_e$ be the roots of Ψ. Then for every $2\leqslant i\leqslant n$ we have $v_p\left(\frac{r_1-r_i}{r_1}\right)\leqslant\frac{1}{p-1}$.*

Proof. Let $E=k(r_1)$. The lemma may be rephrased as a statement about the higher ramification theory of the extension E/k, which need not be Galois; for the ramification theory of non-Galois extensions, see for instance [3, III, Section 3], or the appendix to [2]. In fact, the integers $v_E\left(\frac{r_1-r_i}{r_1}\right)$ are the lower ramification breaks for the extension E/k. The lemma is equivalent to the statement that these breaks are bounded above by $\frac{1}{p-1}\cdot v_E(p)$. Our method is to reduce to the case of a Galois extension, where the lemma is well-known (see for instance [19, Exercise 3(c), p. 72]).

Let $F\subset\Omega$ be the splitting field of Ψ, and set $G=\mathrm{Gal}(F/k)$, $H=\mathrm{Gal}(F/E)$. Let $D=F^{G_1}$ be the fixed field of the wild ramification subgroup of G, let e_1 be the ramification index of D/k, and let e_2 be the ramification index of ED/E. Then $p\nmid e_1$, and hence $p\nmid e_2$. It follows that the Hasse-Herbrand functions for the extensions D/k and ED/E are given by $\phi_{D/k}(x)=x/e_1$ and $\phi_{ED/E}(x)=x/e_2$ for $x\geqslant 0$. Using the composition rule for towers of extensions we get $\phi_{E/k}(x)=\frac{1}{e_1}\phi_{ED/D}(e_2x)$. Since the largest lower ramification break of E/k is $\inf\{x:\phi'_{E/k}(x)=1/e\}$, it suffices to prove the lemma for the extension ED/D. Since $G_1=\mathrm{Gal}(F/D)$ is a p-group, there is a refinement $G_1=G_1^{(0)}\geqslant G_1^{(1)}\geqslant G_1^{(2)}\geqslant\cdots\geqslant G_1^{(n-1)}\geqslant G_1^{(n)}=\{1\}$ of the ramification filtration of G_1 such that $G_1\trianglerighteq G_1^{(i)}$ and $|G_1^{(i)}/G_1^{(i+1)}|=p$ for all $0\leqslant i\leqslant n-1$. Let j be the largest integer such that $G_1^{(j)}$ is not contained in H, and let D' be the subfield of F fixed by $G_1^{(j)}(H\cap G_1)$. Then the largest lower ramification break of ED/D is the same as the largest lower ramification break of ED/D'. Since $|G_1^{(j)}(H\cap G_1)/(H\cap G_1)|=p$, we have $H\cap G_1\trianglelefteq G_1^{(j)}(H\cap G_1)$. Therefore the extension ED/D' is Galois. It follows that the lemma holds for ED/D', and hence also for E/k. □

Let $\mathfrak{C}(p,n,f,e,t)$ be the number of isomorphism classes of finite commutative chain rings with invariants (p,n,f,e,t). Then Proposition 2.1(iii) implies that

$$\mathfrak{C}(p,n,f,e,t)=\mathfrak{I}(\mathbb{Q}_p,f,e) \quad \text{when } (n-1)e+t>\left(\frac{p}{p-1}+v_p(e)\right)e. \tag{2.7}$$

When $p\nmid e$, the number $\mathfrak{C}(p,n,f,e,t)$ was first determined by Clark and Liang [1]. A different formula for this quantity was given in [9].

Theorem 2.3 (Clark and Liang [1] and Hou [9]). *Let p be a prime and let n,f,e,t be positive integers such that $n\geqslant 2$, $1\leqslant t\leqslant e$, and $p\nmid e$. Then*

$$\mathfrak{C}(p,n,f,e,t)=\sum_{c\mid(e,p^f-1)}\frac{\phi(c)}{\tau(c)}=\frac{1}{f}\sum_{i=0}^{f-1}(p^{(i,f)}-1,e), \tag{2.8}$$

where ϕ is the Euler function, (a,b) is the greatest common divisor of a and b, and $\tau(c)$ is the smallest positive integer m such that $p^m\equiv 1 \pmod c$.

From Proposition 2.1(iii) and Theorem 2.3 it follows that when $p\nmid e$,

$$\mathfrak{I}(\mathbb{Q}_p,f,e)=\sum_{c\mid(e,p^f-1)}\frac{\phi(c)}{\tau(c)}=\frac{1}{f}\sum_{i=0}^{f-1}(p^{(i,f)}-1,e). \tag{2.9}$$

In Section 4, we derive a third formula for $\mathfrak{I}(\mathbb{Q}_p,f,e)$ in the case $p\nmid e$. In the other direction, our formulas for $\mathfrak{I}(F,f,e)$ allow us to compute $\mathfrak{C}(p,n,f,e,t)$ in the following two cases (cf. (2.7), Theorem 5.6, and Theorem 10.1):

(i) $p\,||\,e$ and $n>3+\frac{1}{p-1}-\frac{t}{e}$;
(ii) $p>2$, $p^2\,||\,e$, $n>4+\frac{1}{p-1}-\frac{t}{e}$, and $(p^f-1,e)=1$.

3. Preparatory results about p-adic fields

Proposition 3.1. *Let $F\subset K$ be finite extensions of $\mathbb{Q}_p$ such that K/F is totally ramified of degree p^is, with $p\nmid s$. Then for each positive integer $d\mid s$, there is a unique field K_d such that $F\subset K_d\subset K$ and $[K_d:F]=d$. Furthermore, for $d_1\mid s$ and $d_2\mid s$, we have $K_{d_1}\subset K_{d_2}$ if and only if $d_1\mid d_2$.*

Proof. Let L/F be the Galois closure of K/F, and set $G=\mathrm{Gal}(L/F)$ and $H=\mathrm{Gal}(L/K)$. Let G_0 be the inertia subgroup and G_1 the wild inertia subgroup of G (so G_1 is the unique Sylow p-subgroup of G_0). Then G_0/G_1 is a cyclic group whose order is prime to p and divisible by s. Since $|G/H|=p^is$ factors as the product of $|G_1H/H|=|G_1/(G_1\cap H)|$, which is a power of p, and $|G/G_1H|=|G_0/(G_0\cap G_1H)|$,

which is prime to p, we have $|G_0/(G_0 \cap G_1 H)| = s$. Let $N = G_0 \cap G_1 H$. Then N is the unique subgroup of G_0 of index s which contains G_1, so $N \trianglelefteq G$. Since K/F is a totally ramified extension we have $G_0 H = G$. Therefore $G_1 H/N$ maps isomorphically onto G/G_0, and hence G/N is a semidirect product of $G_1 H/N \cong G/G_0$ acting on G_0/N. This implies that for each $d \mid s$ there is a unique subgroup $S_d \leqslant G$ of index d such that $S_d \geqslant G_1 H$. The fixed field of S_d acting on L is K_d. □

Proposition 3.2. *Let F be a finite extension of $\mathbb{Q}_p$ and set $f(F/\mathbb{Q}_p) = f_0$. Let $e = p^i s$ with $p \nmid s$, and let $K \in \mathscr{E}(F, f, e)$.*

(i) *There is a unique field L_K such that $F \subset L_K \subset K$ and K/L_K is totally ramified of degree p^i.*

(ii) *If $(p^{f_0 f} - 1, s) = 1$, there is a unique field E_K such that $F \subset E_K \subset K$ and E_K/F is totally ramified of degree s. Moreover, we have $E_K \subset L_K$ and $\mathrm{Aut}(K/F) = \mathrm{Aut}(K/E_K)$.*

Proof. (i) This is a special case of Proposition 3.1.

(ii) Let k/F be the maximal unramified subextension of K/F. Since $p \nmid s$, there are uniformizers π_{L_K} for L_K and π_F for F such that $\pi_{L_K}^s/\pi_F \in \mathscr{O}_k^\times$ (see [3, II, Proposition 3.5]). Since $((p^{f_0 f} - 1) \cdot p, s) = 1$, we have $\pi_{L_K}^s/\pi_F = \beta^s$ for some $\beta \in \mathscr{O}_k^\times$. Then $(\pi_{L_K}/\beta)^s = \pi_F$, and hence $E_K = F(\pi_{L_K}/\beta)$ is a totally ramified extension of F of degree s which is contained in L_K. To prove the uniqueness of E_K, assume that we have $F \subset E \subset K$ with E/F totally ramified of degree s. Then there is a uniformizer π_E for E such that $\pi_E^s/\pi_F \in \mathscr{O}_k^\times$. As above we get $\delta \in \mathscr{O}_k^\times$ with $\delta^s = \pi_E^s/\pi_F$ and $(\pi_E/\delta)^s = \pi_F = (\pi_{L_K}/\beta)^s$. Thus $\pi_E/\delta = \zeta \pi_{L_K}/\beta$ for some $\zeta \in L_K$ with $\zeta^s = 1$. Since $((p^{f_0 f} - 1) \cdot p, s) = 1$ we must have $\zeta = 1$, and hence $E = k(\pi_E/\delta) = k(\pi/\beta) = E_K$.

To prove the last statement, we note that for any $\sigma \in \mathrm{Aut}(K/F)$ we have $\sigma(E_K) = E_K$ by the uniqueness of E_K. Thus $\sigma|_{E_K} \in \mathrm{Aut}(E_K/F)$. We have already seen that $E_K = F(\pi_{E_K})$ for some $\pi_{E_K} \in E_K$ such that $\pi_{E_K}^s$ is a uniformizer for F. Since F does not contain any nontrivial sth root of unity, it follows that $\mathrm{Aut}(E_K/F) = \{\mathrm{id}\}$. Thus $\sigma \in \mathrm{Aut}(K/E_K)$. □

Let $K/\mathbb{Q}_p$ be a finite extension with $f(K/\mathbb{Q}_p) = f$, $e(K/\mathbb{Q}_p) = e$, and let $\gamma \in \mathrm{Aut}(K/\mathbb{Q}_p)$. Let K^γ denote the subfield of K fixed by $\langle \gamma \rangle$ and put $e(\gamma) = e(K/K^\gamma)$ and $f(\gamma) = f(K/K^\gamma)$. The elementary abelian p-group $V_K = K^\times/(K^\times)^p$ can be viewed as a module over the group ring $\mathbb{F}_p[\langle \gamma \rangle]$, where $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Our approach in Section 5 depends on knowing the $\mathbb{F}_p[\langle \gamma \rangle]$-module structure of V_K in the case $p \nmid e(\gamma)$. The rest of this section is devoted to the determination of this $\mathbb{F}_p[\langle \gamma \rangle]$-module structure. The first step is to factor $K^\times$ as

$$K^\times \cong \langle \pi_K \rangle \times \langle \zeta_{p^f - 1} \rangle \times U_1, \tag{3.1}$$

where $U_1 = 1 + \pi_K \mathscr{O}_K$. We have then

$$V_K \cong (\langle \pi_K \rangle / \langle \pi_K^p \rangle) \times (U_1/U_1^p). \tag{3.2}$$

Let F/K^γ be the maximal unramified subextension of K/K^γ; then F is the fixed field of $\langle \gamma^{f(\gamma)} \rangle$, and K/F is a totally ramified cyclic extension of degree $e(\gamma)$. Since $p \nmid e(\gamma)$, the field F contains an $e(\gamma)$th root of unity, and there is a uniformizer π_K for K such that $\pi_K^{e(\gamma)} \in F$. In fact we have $\pi_K^{e(\gamma)} = \eta\pi$ for some $\eta \in \mathcal{O}_F^\times$ and $\pi \in K^\gamma$. Since $\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^{e(\gamma)}$ is generated by roots of unity, we may assume that η is a root of unity, of order prime to p. It follows that $\gamma(\pi_K^{e(\gamma)}) = \eta^{q^t-1}\pi_K^{e(\gamma)}$, where $t \geqslant 0$ and q is the cardinality of the residue field of K^γ. Since $\eta^{q-1} \in (K^\times)^p$, this implies that γ acts trivially on the image of $\pi_K^{e(\gamma)}$ in V_K, and hence also on the image of π_K in V_K. Since U_1 is clearly stabilized by γ, this implies that the factors in (3.2) are $\mathbb{F}_p[\langle\gamma\rangle]$-submodules of V_K. Thus it remains only to determine the $\mathbb{F}_p[\langle\gamma\rangle]$-module structure of U_1/U_1^p.

Let $o(\gamma)$ denote the order of γ.

Proposition 3.3. (i) *If $\zeta_p \notin K$, there is an isomorphism of $\mathbb{Z}_p[\langle\gamma\rangle]$-modules*

$$U_1 \cong \mathbb{Z}_p[\langle\gamma\rangle]^{n_K/o(\gamma)}. \tag{3.3}$$

Hence there is an isomorphism of $\mathbb{F}_p[\langle\gamma\rangle]$-modules

$$U_1/U_1^p \cong \mathbb{F}_p[\langle\gamma\rangle]^{n_K/o(\gamma)}. \tag{3.4}$$

(ii) *If $\zeta_p \in K$ and $p \nmid e(\gamma)$, there is an isomorphism of $\mathbb{F}_p[\langle\gamma\rangle]$-modules*

$$U_1/U_1^p \cong \langle\zeta_p\rangle \times \mathbb{F}_p[\langle\gamma\rangle]^{n_K/o(\gamma)}. \tag{3.5}$$

Proof. (i) We use Theorem 4(b) in [21]. This theorem implies that as long as U_1 contains no roots of unity, the $\mathbb{Z}_p[\langle\gamma\rangle]$-isomorphism class of U_1 is determined by its $\mathbb{Z}_p$-rank. Since $\langle\gamma\rangle$ is cyclic, this means that we can replace the extension K/K^γ with an extension K'/k' such that K'/k' and $k'/\mathbb{Q}_p$ are unramified, $n_{k'} = n_{K^\gamma}$, and $\mathrm{Gal}(K'/k') \cong \mathrm{Gal}(K/K^\gamma) = \langle\gamma\rangle$. The logarithm gives an isomorphism between the $\mathbb{Z}_p[\mathrm{Gal}(K'/k')]$-modules $U_1' = 1 + p\mathcal{O}_{K'}$ and $p\mathcal{O}_{K'}$. Since K'/k' is unramified, $p\mathcal{O}_{K'}$ is free over $\mathbb{Z}_p[\mathrm{Gal}(K'/k')]$ of rank $n_{K'}/o(\gamma)$. It follows that U_1' is free over $\mathbb{Z}_p[\mathrm{Gal}(K'/k')]$ of rank $n_{K'}/o(\gamma)$, and hence that U_1 is free over $\mathbb{Z}_p[\langle\gamma\rangle]$ of rank $n_K/o(\gamma)$. □

The $\mathbb{Z}_p[\langle\gamma\rangle]$-module structure of U_1 cannot be described as simply when U_1 contains roots of unity. In fact, when $p \nmid e(\gamma)$ it follows from another theorem of Gruenberg and Weiss (Theorem 6.1(a) of [4]) that U_1 is cohomologically trivial as a $\mathbb{Z}_p[\langle\gamma\rangle]$-module. Since the $\mathbb{Z}_p$-torsion subgroup $\langle\zeta_{p^s}\rangle$ of U_1 is not in general cohomologically trivial, $\langle\zeta_{p^s}\rangle$ need not be a direct $\mathbb{Z}_p[\langle\gamma\rangle]$-summand of U_1. Therefore to prove Proposition 3.3(ii), we work directly with U_1/U_1^p.

(ii) The group U_1 has a filtration $U_1 \supset U_2 \supset \cdots$, where $U_i = 1 + \pi_K^i\mathcal{O}_K$. This induces a filtration on U_1/U_1^p whose ith filtrant is $\bar{U}_i = U_iU_1^p/U_1^p$. Put $r = pe/(p-1)$. Since we are assuming $\zeta_p \in K$, we have $(p-1) \mid e$ and hence $r \in \mathbb{Z}$.

Define

$$I = \{i \in \mathbb{Z} : 1 \leqslant i \leqslant r \text{ and } p \nmid i\}. \tag{3.6}$$

Our strategy is to first determine the $\mathbb{F}_p[\langle\gamma\rangle]$-module structure of the quotients $\bar{U}_i/\bar{U}_{i+1}$ for $i \in I$, and then use this information to reconstruct U_1/U_1^p. There are isomorphisms of $\mathbb{F}_p[\langle\gamma\rangle]$-modules

$$\begin{aligned} \bar{U}_i/\bar{U}_{i+1} &\cong U_i U_1^p / U_{i+1} U_1^p \\ &\cong U_i/(U_i \cap (U_{i+1} U_1^p)). \end{aligned} \tag{3.7}$$

For $i \in I$ we have $U_i \cap (U_{i+1} U_1^p) = U_{i+1}$, while if $i \notin I$ and $i \neq r$ we have $U_{i+1} U_1^p \supset U_i$. Therefore if $i \in I$ we have

$$\bar{U}_i/\bar{U}_{i+1} \cong U_i/U_{i+1} \cong \pi_K^i \mathcal{O}_K/\pi_K^{i+1}\mathcal{O}_K, \tag{3.8}$$

while if $i \notin I$ and $i \neq r$ we have $\bar{U}_i/\bar{U}_{i+1} = \{1\}$. Finally, we have $|\bar{U}_r/\bar{U}_{r+1}| = p$ since $|U_1/U_1^p| = p^{fe+1}$, $|I| = e$, and $U_{r+1} \subset U_1^p$.

Lemma 3.4. *Let $i \geqslant 0$ and let $\hat{\gamma}$ denote the automorphism of $\pi_K^i \mathcal{O}_K/\pi_K^{i+1}\mathcal{O}_K$ induced by γ. Then $\hat{\gamma}^0, \hat{\gamma}^1, \ldots, \hat{\gamma}^{f(\gamma)-1}$ are linearly independent over $\bar{K}$.*

Proof. If not then there is a monic polynomial

$$P(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_1 X + a_0 \tag{3.9}$$

of degree $m < f(\gamma)$ in $\bar{K}[X]$ such that $P(\hat{\gamma}) = 0$. We assume that m is as small as possible; then $a_0 \neq 0$, since $\hat{\gamma}$ is invertible. Since $1 \leqslant m < f(\gamma)$, there exists $\alpha \in \bar{K}$ such that $\gamma^m(\alpha) \neq \alpha$. Since $P(\hat{\gamma}) \cdot v = 0$ for all $v \in \pi_K^i \mathcal{O}_K/\pi_K^{i+1}\mathcal{O}_K$, we have $P(\hat{\gamma}) \cdot \alpha v = 0$ for all v as well. This implies that

$$Q(X) = \gamma^m(\alpha)X^m + a_{m-1}\gamma^{m-1}(\alpha)X^{m-1} + \cdots + a_1\gamma(\alpha)X + a_0\alpha \tag{3.10}$$

satisfies $Q(\hat{\gamma}) = 0$. Therefore $R(X) = Q(X) - \gamma^m(\alpha)P(X) \in \bar{K}[X]$ is a polynomial of degree $< m$ with nonzero constant term such that $R(\hat{\gamma}) = 0$. This violates the minimality of m, and therefore proves the lemma. □

It follows from Lemma 3.4 that $\hat{\gamma}^0, \hat{\gamma}^1, \ldots, \hat{\gamma}^{f(\gamma)-1}$ are linearly independent over $\bar{K}^\gamma$, and hence that the degree of the minimal polynomial of $\hat{\gamma}$ over $\bar{K}^\gamma$ is $\geqslant f(\gamma)$. Since $\pi_K^i \mathcal{O}_K/\pi_K^{i+1}\mathcal{O}_K$ has dimension $f(\gamma)$ over $\bar{K}^\gamma$, this implies that $\pi_K^i \mathcal{O}_K/\pi_K^{i+1}\mathcal{O}_K$ is a cyclic $\bar{K}^\gamma[\langle\gamma\rangle]$-module generated by some v_i, i.e.,

$$\pi_K^i \mathcal{O}_K/\pi_K^{i+1}\mathcal{O}_K = \bar{K}^\gamma[\langle\gamma\rangle] \cdot v_i. \tag{3.11}$$

Since $\gamma^{f(\gamma)}$ generates the inertia group of the tamely ramified extension K/K^γ, the image ξ of $\gamma^{f(\gamma)}(\pi_K)/\pi_K$ in $\bar{K}$ is a primitive $e(\gamma)$th root of unity. On the other hand, class field theory gives an onto homomorphism $\rho : (K^\gamma)^\times \to \langle \gamma \rangle$ such that the inertia subgroup $\langle \gamma^{f(\gamma)} \rangle$ of $\langle \gamma \rangle$ is the image of the unit group of K^γ. Hence $(K^\gamma)^\times$ contains an element of order $e(\gamma)$. Therefore $\bar{K}^\gamma$ contains a primitive $e(\gamma)$th root of unity, so we have $\xi \in \bar{K}^\gamma$. In particular, $\bar{K}^\gamma \cdot v_i$ is a $\bar{K}^\gamma[\langle \gamma^{f(\gamma)} \rangle]$-submodule of $\pi_K^i \mathcal{O}_K/\pi_K^{i+1}\mathcal{O}_K$.

Let $\bar{\pi}_K^i$ denote the image of π_K^i in $\pi_K^i \mathcal{O}_K/\pi_K^{i+1}\mathcal{O}_K$. Then $\hat{\gamma}^{f(\gamma)}(\bar{\pi}_K^i) = \xi^i \bar{\pi}_K^i$. Since $\langle \gamma^{f(\gamma)} \rangle$ acts trivially on $\bar{K}^\gamma$, it follows that there is a $\bar{K}^\gamma[\langle \gamma^{f(\gamma)} \rangle]$-module isomorphism

$$\bar{K}^\gamma[\langle \gamma^{f(\gamma)} \rangle] \cong \bigoplus_{i=0}^{e(\gamma)-1} \bar{K}^\gamma \cdot v_i. \tag{3.12}$$

Therefore $\bar{K}^\gamma \cdot v_i$ is a projective $\bar{K}^\gamma[\langle \gamma^{f(\gamma)} \rangle]$-module. Using (3.11) we get

$$\pi_K^i \mathcal{O}_K/\pi_K^{i+1}\mathcal{O}_K \cong \bar{K}^\gamma[\langle \gamma \rangle] \otimes_{\bar{K}^\gamma[\langle \gamma^{f(\gamma)} \rangle]} \bar{K}^\gamma \cdot v_i. \tag{3.13}$$

It follows that $\pi_K^i \mathcal{O}_K/\pi_K^{i+1}\mathcal{O}_K$ is projective over $\bar{K}^\gamma[\langle \gamma \rangle]$, and hence also over $\mathbb{F}_p[\langle \gamma \rangle]$. Using (3.8) we get an $\mathbb{F}_p[\langle \gamma \rangle]$-module isomorphism

$$U_1/U_1^p \cong \left(\bigoplus_{i \in I} \pi_K^i \mathcal{O}/\pi_K^{i+1}\mathcal{O}_K \right) \oplus \bar{U}_r. \tag{3.14}$$

Write $e = dp^t$ with $p \nmid d$; then $e(\gamma) \mid d$ and $(p-1) \mid d$. Partition I into $I \cap [0]$, $I \cap [1], \ldots, I \cap [d-1]$, where $[i]$ is the congruence class of i modulo d. Then each subset $I \cap [i]$ contains either $\frac{e}{d}$, $\frac{e}{d} - 1$, or $\frac{e}{d} + 1$ elements. However, using the fact that $(p-1) \mid d$, one can show that $|I \cap [i]| = \frac{e}{d} \pm 1$ if and only if $|I \cap [pi]| = \frac{e}{d} \mp 1$. If $i \equiv j \pmod{d}$ then there is an $\mathbb{F}_p[\langle \gamma^{f(\gamma)} \rangle]$-module isomorphism $\bar{K}^\gamma \cdot v_i \cong \bar{K}^\gamma \cdot v_j$. On the other hand, if v_{pi} is chosen suitably, $x \mapsto x^p$ gives an $\mathbb{F}_p[\langle \gamma^{f(\gamma)} \rangle]$-module isomorphism between $\bar{K}^\gamma \cdot v_i$ and $\bar{K}^\gamma \cdot v_{pi}$. Therefore we have an $\mathbb{F}_p[\langle \gamma^{f(\gamma)} \rangle]$-module isomorphism

$$\bigoplus_{i \in I} \bar{K}^\gamma \cdot v_i \cong \left(\bigoplus_{i=0}^{d-1} \bar{K}^\gamma \cdot v_i \right)^{e/d}. \tag{3.15}$$

Using (3.12) we get

$$\begin{aligned} \bigoplus_{i \in I} \bar{K}^\gamma \cdot v_i &\cong \left(\bigoplus_{i=0}^{e(\gamma)-1} \bar{K}^\gamma \cdot v_i \right)^{e/e(\gamma)} \\ &\cong \bar{K}^\gamma[\langle \gamma^{f(\gamma)} \rangle]^{e/e(\gamma)} \\ &\cong \mathbb{F}_p[\langle \gamma^{f(\gamma)} \rangle]^{n_K/o(\gamma)}. \end{aligned} \tag{3.16}$$

Therefore by (3.13) and (3.16) there are $\mathbb{F}_p[\langle\gamma\rangle]$-module isomorphisms

$$\begin{aligned}\bigoplus_{i\in I}\pi_K^i\mathcal{O}_K/\pi_K^{i+1}\mathcal{O}_K &\cong \bigoplus_{i\in I}(\bar{K}^\gamma[\langle\gamma\rangle]\otimes_{\bar{K}^\gamma[\langle\gamma^{f(\gamma)}\rangle]}\bar{K}^\gamma\cdot v_i)\\ &\cong \bigoplus_{i\in I}(\mathbb{F}_p[\langle\gamma\rangle]\otimes_{\mathbb{F}_p[\langle\gamma^{f(\gamma)}\rangle]}\bar{K}^\gamma\cdot v_i)\\ &\cong \mathbb{F}_p[\langle\gamma\rangle]\otimes_{\mathbb{F}_p[\langle\gamma^{f(\gamma)}\rangle]}\left(\bigoplus_{i\in I}\bar{K}^\gamma\cdot v_i\right)\\ &\cong \mathbb{F}_p[\langle\gamma\rangle]\otimes_{\mathbb{F}_p[\langle\gamma^{f(\gamma)}\rangle]}\mathbb{F}_p[\langle\gamma^{f(\gamma)}\rangle]^{n_K/o(\gamma)}\\ &\cong \mathbb{F}_p[\langle\gamma\rangle]^{n_K/o(\gamma)}.\end{aligned}\tag{3.17}$$

To complete the proof of Proposition 3.3(ii), we need only determine the $\mathbb{F}_p[\langle\gamma\rangle]$-module structure of $\bar{U}_r$.

Lemma 3.5. *There is an $\mathbb{F}_p[\langle\gamma\rangle]$-module isomorphism $\bar{U}_r\cong\langle\zeta_p\rangle$.*

Proof. Define a group homomorphism $\psi: U_r\to\mathbb{F}_p$ by setting

$$\psi(1+p(\zeta_p-1)x)=\mathrm{Tr}_{\bar{K}/\mathbb{F}_p}(\bar{x}),\tag{3.18}$$

where $x\in\mathcal{O}_K$ and $\bar{x}$ is the image of x in $\bar{K}$. We claim that $\psi(U_r\cap(U_{r+1}U_1^p))=0$. If $y\in U_r\cap(U_{r+1}U_1^p)$, then $y\equiv(1+(\zeta_p-1)z)^p\pmod{\pi_K^{r+1}}$ for some $z\in\mathcal{O}_K$. We have

$$(1+(\zeta_p-1)z)^p\equiv 1+p(\zeta_p-1)\left(z+\frac{(\zeta_p-1)^{p-1}}{p}z^p\right)\pmod{\pi_K^{r+1}}.\tag{3.19}$$

Since $(\zeta_p-1)^{p-1}\equiv -p\pmod{p\pi_K}$, we have

$$\mathrm{Tr}_{\bar{K}/\mathbb{F}_p}\left(\bar{z}+\overline{\frac{(\zeta_p-1)^{p-1}}{p}z^p}\right)=\mathrm{Tr}_{\bar{K}/\mathbb{F}_p}(\bar{z}-\bar{z}^p)=0,\tag{3.20}$$

so $\psi(y)=0$. Since ψ is nontrivial, it follows that ψ induces a group isomorphism between $\bar{U}_r\cong U_r/(U_r\cap(U_{r+1}U_1^p))$ and $\mathbb{F}_p$. Suppose that $\gamma(\zeta_p)=\zeta_p^m$. Then

$$\begin{aligned}\gamma(1+p(\zeta_p-1)z)&=1+p(\zeta_p^m-1)\gamma(z)\\ &=1+p(\zeta_p-1)(1+\cdots+\zeta_p^{m-1})\gamma(z)\\ &\equiv 1+p(\zeta_p-1)m\gamma(z)\pmod{\pi_K^{r+1}}.\end{aligned}\tag{3.21}$$

Since $\mathrm{Tr}_{\bar{K}/\mathbb{F}_p}(\overline{m\gamma(z)})=m\mathrm{Tr}_{\bar{K}/\mathbb{F}_p}(\bar{z})$, we see that γ acts on $\bar{U}_r\cong\mathbb{F}_p$ by raising to the power m. Therefore the $\mathbb{F}_p[\langle\gamma\rangle]$-modules $\bar{U}_r$ and $\langle\zeta_p\rangle$ are isomorphic. □

Using (3.14), (3.17), and Lemma 3.5, we get an $\mathbb{F}_p[\langle\gamma\rangle]$-module isomorphism

$$U_1/U_1^p \cong \langle\zeta_p\rangle \times \mathbb{F}_p[\langle\gamma\rangle]^{n_K/o(\gamma)}, \tag{3.22}$$

and the proof of Proposition 3.3(ii) is complete. □

Corollary 3.6. (i) *If $\zeta_p \notin K$, there is an isomorphism of $\mathbb{F}_p[\langle\gamma\rangle]$-modules*

$$K^\times/(K^\times)^p \cong \mathbb{F}_p \times \mathbb{F}_p[\langle\gamma\rangle]^{n_K/o(\gamma)}. \tag{3.23}$$

(ii) *If $\zeta_p \in K$ and $p \nmid e(\gamma)$, there is an isomorphism of $\mathbb{F}_p[\langle\gamma\rangle]$-modules*

$$K^\times/(K^\times)^p \cong \mathbb{F}_p \times \langle\zeta_p\rangle \times \mathbb{F}_p[\langle\gamma\rangle]^{n_K/o(\gamma)}. \tag{3.24}$$

4. The case $p \nmid e$

In this section we determine $\mathfrak{I}(F,f,e)$ in the cases where $p \nmid e$. Thus we are restricting our attention to tamely ramified extensions of the p-adic field F, which are in general well-understood. Therefore we only give outlines for the arguments in this section, most of which are not new. Besides calculating $\mathfrak{I}(F,f,e)$, we also collect some facts about tamely ramified extensions of F which will be useful in the next section.

We start by listing the elements of $\mathscr{E}(F,f,e)$. Let q denote the cardinality of the residue field of F and set $g = (q^f - 1)e$. Let π_F be a uniformizer of F, let $\pi_E \in \Omega$ be an eth root of π_F, and define $E = F(\zeta_g, \pi_E)$. The extension E/F is Galois, with

$$\mathrm{Gal}(E/F) = \langle \boldsymbol{\sigma}, \boldsymbol{\tau} : \boldsymbol{\sigma}^e = \boldsymbol{\tau}^{df} = 1, \boldsymbol{\tau}\boldsymbol{\sigma}\boldsymbol{\tau}^{-1} = \boldsymbol{\sigma}^q \rangle, \tag{4.1}$$

where $df = [F(\zeta_g) : F]$. The actions of $\boldsymbol{\sigma}$ and $\boldsymbol{\tau}$ on E are given by

$$\boldsymbol{\sigma}(\pi_E) = \zeta_e\pi_E, \quad \boldsymbol{\sigma}(\zeta_g) = \zeta_g, \quad \boldsymbol{\tau}(\pi_E) = \pi_E, \quad \boldsymbol{\tau}(\zeta_g) = \zeta_g^q. \tag{4.2}$$

For $0 \leqslant h < e$, we define $K_h = F(\zeta_{q^f-1}, \pi_h)$, where $\pi_h = \zeta_g^h\pi_E$; equivalently, K_h is the subfield of E fixed by $\langle \boldsymbol{\sigma}^{-h}\boldsymbol{\tau}^f \rangle$. Then we have

$$\mathscr{E}(F,f,e) = \{K_h : 0 \leqslant h < e\}. \tag{4.3}$$

We now describe the F-automorphisms of K_h. The inertia subgroup $\mathrm{Aut}(K_h/F(\zeta_{q^f-1}))$ of $\mathrm{Aut}(K_h/F)$ is a cyclic group of order $b = (e, q^f - 1)$ generated

by an element $\boldsymbol{\mu}$ such that $\boldsymbol{\mu}(\zeta_{q^f-1}) = \zeta_{q^f-1}$ and $\boldsymbol{\mu}(\pi_h) = \zeta_b \pi_h$. We need to determine which elements of $\mathrm{Gal}(F(\zeta_{q^f-1})/F)$ can be extended to automorphisms of K_h. Let $\boldsymbol{\rho}$ be the Frobenius automorphism of $F(\zeta_{q^f-1})/F$. For $c \geqslant 0$ we attempt to extend $\boldsymbol{\rho}^c$ to an element $\boldsymbol{\nu}_c$ of $\mathrm{Aut}(K_h/F)$. Since $\pi_h^g = \pi_E^g = \pi_F^{q^f-1} \in F$, we have $\boldsymbol{\nu}_c(\pi_h) = \varepsilon \pi_h$ for some $\varepsilon \in K_h$ such that $\varepsilon^g = 1$. But since $p \nmid g$, we must have $\varepsilon = \zeta_{q^f-1}^x$ for some $x \in \mathbb{Z}$. Therefore

$$\zeta_{q^f-1}^{ex+h} \pi_F = (\zeta_{q^f-1}^x \pi_h)^e = \boldsymbol{\nu}_c(\pi_h)^e = \boldsymbol{\nu}_c(\pi_h^e) = \boldsymbol{\nu}_c(\zeta_{q^f-1}^h \pi_F) = \zeta_{q^f-1}^{hq^c} \pi_F, \tag{4.4}$$

which implies that

$$ex \equiv (q^c - 1)h \,(\mathrm{mod}\, q^f - 1). \tag{4.5}$$

Conversely, if x satisfies (4.5), then $\boldsymbol{\rho}^c$ can be extended to $\boldsymbol{\nu}_c \in \mathrm{Aut}(K_h/F)$ such that $\boldsymbol{\nu}_c(\pi_h) = \zeta_{q^f-1}^x \pi_h$.

Congruence (4.5) can be solved for x if and only if $b = (e, q^f - 1)$ divides $(q^c - 1)h$. Let c_h be the smallest positive integer c satisfying this condition. Then c_h is the order of q in $\left(\mathbb{Z}/\frac{b}{(b,h)}\mathbb{Z}\right)^\times$. Let $u \in \mathbb{Z}$ satisfy $eu \equiv b \,(\mathrm{mod}\, q^f - 1)$ and set $m_h = \frac{1}{b}(q^{c_h} - 1)hu$. Then $x = m_h$ is a solution to (4.5) with $c = c_h$.

The elements in $\mathrm{Gal}(F(\zeta_{q^f-1})/F)$ which can be extended to automorphisms of K_h/F are $(\boldsymbol{\rho}^{c_h})^i$ for $0 \leqslant i < f/c_h$. Let $\boldsymbol{\nu} \in \mathrm{Aut}(K_h/F)$ be the extension of $\boldsymbol{\rho}^{c_h}$ defined by $\boldsymbol{\nu}(\pi_h) = \zeta_{q^f-1}^{m_h} \pi_h$. Then $\boldsymbol{\nu}$ generates the group

$$\mathrm{Aut}(K_h/F)/\mathrm{Gal}(F(\zeta_{q^f-1})/F) = \mathrm{Aut}(K_h/F)/\langle \boldsymbol{\mu} \rangle \tag{4.6}$$

and satisfies $\boldsymbol{\nu}^{f/c_h} \in \langle \boldsymbol{\mu} \rangle$. The actions of $\boldsymbol{\mu}$ and $\boldsymbol{\nu}$ on $K_h = F(\zeta_{q^f-1}, \pi_h)$ are given by

$$\boldsymbol{\mu}(\zeta_{q^f-1}) = \zeta_{q^f-1}, \quad \boldsymbol{\mu}(\pi_h) = \zeta_b \pi_h, \quad \boldsymbol{\nu}(\zeta_{q^f-1}) = \zeta_{q^f-1}^{q^{c_h}}, \quad \boldsymbol{\nu}(\pi_h) = \zeta_{q^f-1}^{m_h} \pi_h. \tag{4.7}$$

Using (4.7) we find that $\boldsymbol{\nu}^{f/c_h} = \boldsymbol{\mu}^{uh}$ and $\boldsymbol{\nu}\boldsymbol{\mu}\boldsymbol{\nu}^{-1} = \boldsymbol{\mu}^{q^{c_h}}$. Therefore

$$\mathrm{Aut}(K_h/F) = \langle \boldsymbol{\mu}, \boldsymbol{\nu} : \boldsymbol{\mu}^b = 1,\ \boldsymbol{\nu}^{f/c_h} = \boldsymbol{\mu}^{uh},\ \boldsymbol{\nu}\boldsymbol{\mu}\boldsymbol{\nu}^{-1} = \boldsymbol{\mu}^{q^{c_h}} \rangle. \tag{4.8}$$

In particular, $|\mathrm{Aut}(K_h/F)| = bf/c_h$. Combining this fact with (1.3), we get the following proposition.

Proposition 4.1. *Assume that $p \nmid e$. Then*

$$\mathfrak{I}(F,f,e) = \frac{b}{e} \sum_{h=0}^{e-1} \frac{1}{c_h}, \tag{4.9}$$

where $b = (e, q^f - 1)$, q is the cardinality of the residue field of F, and c_h is the smallest positive integer such that b divides $(q^{c_h} - 1)h$.

Remark 4.2. The method of Corollary 4.3 in [9] gives the alternative formula

$$\mathfrak{I}(F,f,e) = \frac{1}{f} \sum_{i=0}^{f-1} (q^{(i,f)} - 1, e). \tag{4.10}$$

On the other hand, Proposition 4.1 with $F = \mathbb{Q}_p$ gives a third formula (in addition to those in Theorem 2.3) for $\mathfrak{C}(p,n,f,e,t)$ when $p \nmid e$ and $n \geqslant 2$,

$$\mathfrak{C}(p,n,f,e,t) = \frac{b}{e} \sum_{h=0}^{e-1} \frac{1}{c_h}. \tag{4.11}$$

Remark 4.3. For future use we note that $\boldsymbol{\mu}$ is the restriction to K_h of $\boldsymbol{\sigma}^{e/b}$ and $\boldsymbol{\nu}$ is the restriction to K_h of $\boldsymbol{\sigma}^{v_h}\boldsymbol{\tau}^{c_h}$, where

$$v_h = \frac{em_h + h(1 - q^{c_h})}{q^f - 1}. \tag{4.12}$$

For each $\gamma \in \mathrm{Aut}(K_h/F)$, let K_h^{γ} denote the subfield of K_h fixed by $\langle \gamma \rangle$. By (4.8), we can write γ uniquely in the form $\gamma = \boldsymbol{\mu}^i \boldsymbol{\nu}^j$ with $0 \leqslant i < b$ and $0 \leqslant j < f/c_h$. The smallest power of γ which lies in the inertia subgroup $\langle \boldsymbol{\mu} \rangle$ of $\mathrm{Aut}(K_h/F)$ is

$$\gamma^{\frac{f}{(f,c_h j)}} = (\boldsymbol{\mu}^i \boldsymbol{\nu}^j)^{\frac{f}{(f,c_h j)}} = \boldsymbol{\mu}^{t(\gamma)}, \tag{4.13}$$

where $t(\gamma)$ is computed using (4.8) to be

$$t(\gamma) = \frac{q^{\mathrm{lcm}(f,c_h j)} - 1}{q^{c_h j} - 1} \cdot i + \frac{uhc_h j}{(f, c_h j)}. \tag{4.14}$$

This implies that the extension K_h/K_h^{γ} has residue degree $f(\gamma) = f/(f, c_h j)$ and ramification index $e(\gamma) = b/(b, t(\gamma))$. The order $o(\gamma) = [K_h : K_h^{\gamma}]$ of γ is given by

$$o(\gamma) = e(\gamma) \cdot f(\gamma) = \frac{b}{(b, t(\gamma))} \cdot \frac{f}{(f, c_h j)}. \tag{4.15}$$

5. The case $p \,||\, e$

In this section we assume $e = pe_0$ with $p \nmid e_0$. We use the notation of Section 4 with e_0 in place of e. In particular,

$$\begin{cases} q = \text{the cardinality of the residue class field of } F, \\ g = (q^f - 1)e_0, \\ b = (e_0, q^f - 1), \\ c_h = \text{the smallest positive integer such that } b \mid (q^{c_h} - 1)h, \\ u \in \mathbb{Z} \text{ satisfies } e_0 u \equiv b \pmod{q^f - 1}, \\ m_h = \dfrac{(q^{c_h} - 1)h}{b} u, \\ v_h = \dfrac{e_0 m_h + h(1 - q^{c_h})}{q^f - 1}. \end{cases} \tag{5.1}$$

Let $L \in \mathscr{E}(F, f, e)$. Then by Proposition 3.1, there is a unique $K \in \mathscr{E}(F, f, e_0)$ which is contained in L. It follows from (1.3) and (4.3) that

$$\begin{aligned} \mathfrak{I}(F, f, e) &= \frac{1}{fe} \sum_{K \in \mathscr{E}(F,f,e_0)} \sum_{L \in \mathscr{E}(K,1,p)} |\mathrm{Aut}(L/F)| \\ &= \frac{1}{fe} \sum_{h=0}^{e_0 - 1} \sum_{L \in \mathscr{E}(K_h,1,p)} |\mathrm{Aut}(L/F)|. \end{aligned} \tag{5.2}$$

For the time being, we fix $K = K_h$ and concentrate on evaluating the inner sum of (5.2).

Let $L \in \mathscr{E}(K, 1, p)$. Then since $K \in \mathscr{E}(F, f, e_0)$ is uniquely determined by L, restriction induces a homomorphism $\mathrm{Aut}(L/F) \to \mathrm{Aut}(K/F)$. Let $H_L \subset \mathrm{Aut}(K/F)$ be the image of this homomorphism. Then $\mathrm{Aut}(L/F)$ is an extension of H_L by $\mathrm{Aut}(L/K)$. Thus if L/K is not Galois then $\mathrm{Aut}(K/F) = H_L$, while if L/K is Galois then $\mathrm{Aut}(K/F)$ is an extension of H_L by a cyclic group of order p. For each $\gamma \in \mathrm{Aut}(K/F)$, let

$$S_1(\gamma) = \{L \in \mathscr{E}(K, 1, p) : \gamma \in H_L \text{ and } L/K \text{ is Galois}\}, \tag{5.3}$$

$$S_2(\gamma) = \{L \in \mathscr{E}(K, 1, p) : \gamma \in H_L \text{ and } L/K \text{ is not Galois}\}, \tag{5.4}$$

and define $m_i(\gamma) = |S_i(\gamma)|$. Then by counting the elements in the set

$$\{(L, \delta) : L \in \mathscr{E}(K, 1, p),\ \delta \in \mathrm{Aut}(L/F)\} \tag{5.5}$$

in two different ways we find that

$$\sum_{L\in\mathscr{E}(K,1,p)} |\mathrm{Aut}(L/F)| = \sum_{\gamma\in\mathrm{Aut}(K/F)} (p\cdot m_1(\gamma)+m_2(\gamma)). \tag{5.6}$$

Lemma 5.1. *Let $\gamma\in\mathrm{Aut}(K/F)$, let K^γ be the subfield of K/F fixed by $\langle\gamma\rangle$, and let $d(\gamma)=(o(\gamma),p-1)$. Then*

$$m_1(\gamma)=\begin{cases} (d(\gamma)-1)\dfrac{p^{\frac{n_Fe_0f}{o(\gamma)}}-1}{p-1}+\dfrac{p^{\frac{n_Fe_0f}{o(\gamma)}+1}-1}{p-1}-1 & \text{if } \zeta_p\notin K,\\ (d(\gamma)-2)\dfrac{p^{\frac{n_Fe_0f}{o(\gamma)}}-1}{p-1}+2\cdot\dfrac{p^{\frac{n_Fe_0f}{o(\gamma)}+1}-1}{p-1}-1 & \text{if } \zeta_p\in K\backslash K^\gamma,\\ (d(\gamma)-1)\dfrac{p^{\frac{n_Fe_0f}{o(\gamma)}}-1}{p-1}+\dfrac{p^{\frac{n_Fe_0f}{o(\gamma)}+2}-1}{p-1}-1 & \text{if } \zeta_p\in K^\gamma. \end{cases} \tag{5.7}$$

Proof. By class field theory, cyclic extensions L/K of degree p such that $\gamma\in H_L$ correspond to $\langle\gamma\rangle$-invariant subgroups of $V_K=K^\times/(K^\times)^p$ of index p. The unramified degree-p extension of K is excluded from $S_1(\gamma)$, and so $m_1(\gamma)$ is one less than the number of $\langle\gamma\rangle$-invariant subgroups of V_K of index p.

For each of the $d(\gamma)$ homomorphisms $\psi:\langle\gamma\rangle\to\mathbb{F}_p^\times$, the largest quotient on which $\langle\gamma\rangle$ acts through ψ is $V_K(\psi)=V_K/(\gamma-\psi(\gamma))V_K$. On the other hand, if H is a $\langle\gamma\rangle$-invariant subgroup of V_K of index p then $\langle\gamma\rangle$ acts on V_K/H through some homomorphism $\psi:\langle\gamma\rangle\to\mathbb{F}_p^\times$. Thus $H\geqslant(\gamma-\psi(\gamma))V_K$ and $H/(\gamma-\psi(\gamma))V_K$ is a subgroup of $V_K(\psi)$ of index p. In fact, $H\leftrightarrow H/(\gamma-\psi(\gamma))V_K$ gives a one-to-one correspondence between the set of $\langle\gamma\rangle$-invariant subgroups of V_K of index p and the set

$$\bigcup_{\psi:\langle\gamma\rangle\to\mathbb{F}_p^\times}\{U\subset V_K(\psi):[V_K(\psi):U]=p\}. \tag{5.8}$$

If $\zeta_p\notin K$, it follows from Corollary 3.6(i) that there is an isomorphism of $\mathbb{F}_p[\langle\gamma\rangle]$-modules $V_K\cong\mathbb{F}_p\times\mathbb{F}_p[\langle\gamma\rangle]^{\frac{n_Fe_0f}{o(\gamma)}}$. Thus $\dim_{\mathbb{F}_p}V_K(\psi)=\frac{1}{o(\gamma)}n_Fe_0f$ for $\psi\neq1$, and $\dim_{\mathbb{F}_p}V_K(1)=\frac{1}{o(\gamma)}n_Fe_0f+1$. The formula for $m_1(\gamma)$ in the case $\zeta_p\notin K$ follows from this.

Now assume $\zeta_p\in K$. By Corollary 3.6(ii) we have $V_K\cong\mathbb{F}_p\times\langle\zeta_p\rangle\times\mathbb{F}_p[\langle\gamma\rangle]^{\frac{n_Fe_0f}{o(\gamma)}}$. If $\zeta_p\notin K^\gamma$ then $\gamma(\zeta_p)=\zeta_p^m$ for some $m\not\equiv1\pmod p$. Therefore $\dim_{\mathbb{F}_p}V_K(\psi)=\frac{1}{o(\gamma)}n_Fe_0f$ when $\psi(\gamma)\notin\{1,m\}$, and $\dim_{\mathbb{F}_p}V_K(\psi)=\frac{1}{o(\gamma)}n_Fe_0f+1$ when $\psi(\gamma)\in\{1,m\}$. In the case where $\zeta_p\in K^\gamma$ we have $\dim_{\mathbb{F}_p}V_K(\psi)=\frac{1}{o(\gamma)}n_Fe_0f$ when $\psi(\gamma)\neq1$ and

$\dim_{\mathbb{F}_p} V_K(\psi) = \frac{1}{o(\gamma)} n_F e_0 f + 2$ when $\psi(\gamma) = 1$. The remaining formulas for $m_1(\gamma)$ follow from these observations. □

Lemma 5.2. *We have*

$$m_2(\gamma) = \begin{cases} p^{\frac{n_F e_0 f}{o(\gamma)}+2} - p^2 + p - pd(\gamma) \cdot \dfrac{p^{\frac{n_F e_0 f}{o(\gamma)}} - 1}{p-1} & \text{if } \zeta_p \notin K, \\ (p^2-p)p^{\frac{n_F e_0 f}{o(\gamma)}} - p^2 + p - pd(\gamma) \cdot \dfrac{p^{\frac{n_F e_0 f}{o(\gamma)}} - 1}{p-1} & \text{if } \zeta_p \in K. \end{cases} \tag{5.9}$$

Proof. Suppose $L \in S_2(\gamma)$. Since $\mathrm{Aut}(L/F) \cong H_L$, there is a unique $\tilde{\gamma} \in \mathrm{Aut}(L/F)$ which extends γ. Let $L^{\tilde{\gamma}}$ be the subfield of L fixed by $\langle \tilde{\gamma} \rangle$. Then $L^{\tilde{\gamma}}/K^{\gamma}$ is a ramified extension of degree p such that $L^{\tilde{\gamma}}K = L$. Conversely, let M/K^{γ} be a ramified extension of degree p such that the compositum MK is not Galois over K. Then M and K are linearly disjoint over K^{γ} and so $\gamma \in \mathrm{Gal}(K/K^{\gamma})$ can be uniquely extended to an element $\tilde{\gamma} \in \mathrm{Aut}(MK/M)$. Therefore $MK \in S_2(\gamma)$. Thus $M \leftrightarrow MK$ gives a bijection between the set $\{M \in \mathscr{E}(K^{\gamma}, 1, p) : MK/K \text{ not Galois}\}$ and $S_2(\gamma)$. Let

$$\mathscr{Y}(\gamma) = \{M \in \mathscr{E}(K^{\gamma}, 1, p) : M/K^{\gamma} \text{ is Galois}\} \tag{5.10}$$

$$\mathscr{Z}(\gamma) = \{M \in \mathscr{E}(K^{\gamma}, 1, p) : M/K^{\gamma} \text{ is not Galois but } MK/K \text{ is Galois}\}. \tag{5.11}$$

Then we have

$$m_2(\gamma) = |\mathscr{E}(K^{\gamma}, 1, p)| - |\mathscr{Y}(\gamma)| - |\mathscr{Z}(\gamma)|. \tag{5.12}$$

By Krasner's formula (1.1) we have

$$|\mathscr{E}(K^{\gamma}, 1, p)| = p^{\frac{n_F e_0 f}{o(\gamma)}+2} - p^2 + p, \tag{5.13}$$

and by class field theory we have

$$|\mathscr{Y}(\gamma)| = \begin{cases} \dfrac{p^{\frac{n_F e_0 f}{o(\gamma)}+1} - 1}{p-1} - 1 & \text{if } \zeta_p \notin K^{\gamma}, \\ \dfrac{p^{\frac{n_F e_0 f}{o(\gamma)}+2} - 1}{p-1} - 1 & \text{if } \zeta_p \in K^{\gamma}. \end{cases} \tag{5.14}$$

It remains to determine $|\mathscr{Z}(\gamma)|$. Let $M \in \mathscr{Z}(\gamma)$. Then $\gamma \in \mathrm{Gal}(K/K^{\gamma})$ lifts to $\tilde{\gamma} \in \mathrm{Gal}(MK/M)$, so MK/K^{γ} is Galois and $\mathrm{Gal}(MK/K^{\gamma})$ is the semidirect product of $\mathrm{Gal}(MK/M) = \langle \tilde{\gamma} \rangle$ acting on $\mathrm{Gal}(MK/K) \cong \mathbb{Z}/p\mathbb{Z}$. This action is nontrivial since M/K^{γ} is not Galois. On the other hand, suppose that L/K is a cyclic extension of degree p such that L/K^{γ} is Galois and $\mathrm{Gal}(L/K^{\gamma})$ is nonabelian. Then γ can be lifted

to an automorphism $\tilde{\gamma}$ of L, which must satisfy $o(\tilde{\gamma}) = o(\gamma)$, since otherwise $\mathrm{Gal}(L/K^\gamma) = \langle \tilde{\gamma} \rangle$ is abelian. Therefore $\mathrm{Gal}(L/K^\gamma)$ is a semidirect product of $\langle \tilde{\gamma} \rangle$ acting nontrivially on $\mathrm{Gal}(L/K)$. For such an L, the group $\mathrm{Gal}(L/K^\gamma)$ contains p different subgroups which map isomorphically onto $\mathrm{Gal}(K/K^\gamma)$, so there are p elements $M \in \mathscr{L}(\gamma)$ such that $MK = L$. Therefore we have $|\mathscr{L}(\gamma)| = p|\mathscr{W}(\gamma)|$, where

$$\mathscr{W}(\gamma) = \{L : K \subset L \subset \Omega,\ [L : K] = p,\ L/K^\gamma \text{ is Galois and nonabelian}\}. \tag{5.15}$$

By class field theory, elements in $\mathscr{W}(\gamma)$ correspond to subgroups $H \leqslant V_K$ of index p such that H is invariant under the action of $\langle \gamma \rangle$ and such that $\langle \gamma \rangle$ acts nontrivially on V_K/H. Using Corollary 3.6, we find that

$$|\mathscr{W}(\gamma)| = \begin{cases} (d(\gamma) - 1)\dfrac{p^{\frac{n_F e_0 f}{o(\gamma)}} - 1}{p - 1} & \text{if } \zeta_p \notin K \text{ or } \zeta_p \in K^\gamma, \\ (d(\gamma) - 2)\dfrac{p^{\frac{n_F e_0 f}{o(\gamma)}} - 1}{p - 1} + \dfrac{p^{\frac{n_F e_0 f}{o(\gamma)}+1} - 1}{p - 1} & \text{if } \zeta_p \in K \text{ but } \zeta_p \notin K^\gamma. \end{cases} \tag{5.16}$$

Eq. (5.9) now follows from (5.12)–(5.16). □

It follows from Lemmas 5.1 and 5.2 that

$$p \cdot m_1(\gamma) + m_2(\gamma) = \begin{cases} (p^2 + p)p^{\frac{n_F e_0 f}{o(\gamma)}} - p^2 & \text{if } \zeta_p \notin K^\gamma, \\ 2p^{\frac{n_F e_0 f}{o(\gamma)}+2} - p^2 & \text{if } \zeta_p \in K^\gamma. \end{cases} \tag{5.17}$$

In order to write down explicit formulas for $\sum_{L \in \mathscr{E}(K,1,p)} |\mathrm{Aut}(L/F)|$, we change notation slightly: We restore the subscript h to K, and instead of $o(\gamma)$, $t(\gamma)$, K^γ, we write $o(h,i,j)$, $t(h,i,j)$, K_h^{ij}, where $\gamma = \mu^i \nu^j$. If $\zeta_p \notin K_h$, then by combining (5.6) with (5.17) we get the following result.

Proposition 5.3. *If $\zeta_p \notin K_h$ then*

$$\begin{aligned} \sum_{L \in \mathscr{E}(K_h,1,p)} |\mathrm{Aut}(L/F)| &= \sum_{i=0}^{b-1} \sum_{j=0}^{\frac{f}{c_h}-1} ((p^2 + p)p^{\frac{n_F e_0 f}{o(h,i,j)}} - p^2) \\ &= -\frac{p^2 bf}{c_h} + (p^2 + p) \sum_{i=0}^{b-1} \sum_{j=0}^{\frac{f}{c_h}-1} p^{\frac{n_F e_0 f}{o(h,i,j)}}, \end{aligned} \tag{5.18}$$

where

$$o(h,i,j) = \frac{f}{(f, c_h j)} \cdot \frac{b}{(b, t(h,i,j))}, \tag{5.19}$$

$$t(h,i,j)=\frac{q^{\mathrm{lcm}(f,c_h j)}-1}{q^{c_h j}-1}\,i+\frac{uhc_h j}{(f,c_h j)}. \tag{5.20}$$

In order to evaluate (5.2), we need to be able to tell when $\zeta_p\in K_h$, and when $\zeta_p\in K_h^{ij}$. Let f_p be the residue degree and e_p the ramification index of the extension $F(\zeta_p)/F$. A necessary condition for K_h to contain ζ_p is that $f_p\,|\,f$ and $e_p\,|\,e_0$. Therefore, in what follows, we will assume $f_p\,|\,f$ and $e_p\,|\,e_0$. Then $E=F(\zeta_g,\pi_E)$ contains all the fields in $\mathscr{E}(F,f_p,e_p)$, including $F(\zeta_p)$. Therefore $F(\zeta_p)$ is the fixed field of a normal subgroup H of $\mathrm{Gal}(E/F)$. Since the residue degree of $E/F(\zeta_p)$ is f/f_p, and the ramification index is e/e_p, we easily see that $H=\langle\boldsymbol{\sigma}^{e_p},\boldsymbol{\sigma}^l\boldsymbol{\tau}^{f_p}\rangle$ for some l. The following lemma shows that we can assume $l=1$.

Lemma 5.4. *There is an automorphism Ψ of $\mathrm{Gal}(E/F)=\langle\boldsymbol{\sigma},\boldsymbol{\tau}\rangle$ such that*

(i) *Ψ maps the inertia group $\langle\boldsymbol{\sigma}\rangle$ onto itself.*
(ii) *Ψ acts trivially on the quotient $\mathrm{Gal}(E/F)/\langle\boldsymbol{\sigma}\rangle$.*
(iii) *$\Psi(H)=\langle\boldsymbol{\sigma}^{e_p},\boldsymbol{\sigma}\boldsymbol{\tau}^{f_p}\rangle$.*

Proof. Since $\mathrm{Gal}(E/F)/H\cong\mathrm{Gal}(F(\zeta_p)/F)$ is cyclic, it is generated by $\boldsymbol{\sigma}^a\boldsymbol{\tau}$ for some $a\in\mathbb{Z}$. Define an automorphism Ψ_1 of $\mathrm{Gal}(E/F)$ by setting $\Psi_1(\boldsymbol{\sigma})=\boldsymbol{\sigma}$ and $\Psi_1(\boldsymbol{\tau})=\boldsymbol{\sigma}^{-a}\boldsymbol{\tau}$. Then $\Psi_1(H)=\langle\boldsymbol{\sigma}^{e_p},\boldsymbol{\sigma}^d\boldsymbol{\tau}^{f_p}\rangle$, where

$$d=l-\frac{q^{f_p}-1}{q-1}\,a. \tag{5.21}$$

Furthermore, $\boldsymbol{\tau}=\Psi_1(\boldsymbol{\sigma}^a\boldsymbol{\tau})$ generates the quotient $\mathrm{Gal}(E/F)/\Psi_1(H)$. This implies that $(e_p,d)=1$, so there is $k\in\mathbb{Z}$ such that $dk\equiv 1\,(\mathrm{mod}\,e_p)$. In addition, since the homomorphism $(\mathbb{Z}/e_0\mathbb{Z})^\times\to(\mathbb{Z}/e_p\mathbb{Z})^\times$ is onto, we may choose k so that $(e_0,k)=1$. Define an automorphism Ψ_2 of $\mathrm{Gal}(E/F)$ by setting $\Psi_2(\boldsymbol{\sigma})=\boldsymbol{\sigma}^k$ and $\Psi_2(\boldsymbol{\tau})=\boldsymbol{\tau}$. Then $\Psi=\Psi_2\circ\Psi_1$ satisfies the given conditions. □

By Lemma 5.4 we have $H=\langle(\boldsymbol{\sigma}^s)^{e_p},\boldsymbol{\sigma}^s(\boldsymbol{\sigma}^t\boldsymbol{\tau})^{f_p}\rangle$ for some $s,t\in\mathbb{Z}$ such that $(s,e_0)=1$. Let $\tilde{\boldsymbol{\sigma}}=\boldsymbol{\sigma}^s$, $\tilde{\boldsymbol{\tau}}=\boldsymbol{\sigma}^t\boldsymbol{\tau}$, $\tilde{\pi}_E=\zeta_{e_0(q-1)}^{-t}\pi_E$, and $\tilde{\pi}_F=\zeta_{q-1}^{-t}\pi_F$. Then $\tilde{\pi}_F$ is a uniformizer of F and $\tilde{\pi}_E^{e_0}=\tilde{\pi}_F$. Furthermore,

$$\tilde{\boldsymbol{\sigma}}(\tilde{\pi}_E)=\zeta_e^s\tilde{\pi}_E,\quad \tilde{\boldsymbol{\sigma}}(\zeta_g)=\zeta_g,\quad \tilde{\boldsymbol{\tau}}(\tilde{\pi}_E)=\tilde{\pi}_E,\quad \tilde{\boldsymbol{\tau}}(\zeta_g)=\zeta_g^q. \tag{5.22}$$

It follows that by replacing π_F, π_E, $\boldsymbol{\sigma}$, $\boldsymbol{\tau}$ with $\tilde{\pi}_F$, $\tilde{\pi}_E$, $\tilde{\boldsymbol{\sigma}}$, $\tilde{\boldsymbol{\tau}}$ we may assume that $H=\langle\boldsymbol{\sigma}^{e_p},\boldsymbol{\sigma}\boldsymbol{\tau}^{f_p}\rangle$. Under this assumption, for every $x,y\in\mathbb{Z}$ the element $\boldsymbol{\sigma}^x\boldsymbol{\tau}^y$ fixes ζ_p if and only if $\boldsymbol{\sigma}^x\boldsymbol{\tau}^y\in\langle\boldsymbol{\sigma}^{e_p},\boldsymbol{\sigma}\boldsymbol{\tau}^{f_p}\rangle$. By (4.1) this is equivalent to $f_p\,|\,y$ and

$$x\equiv\frac{q^y-1}{q^{f_p}-1}\,(\mathrm{mod}\,e_p). \tag{5.23}$$

Since K_h is the subfield of E fixed by $\langle \boldsymbol{\sigma}^{-h}\boldsymbol{\tau}^f \rangle$, we see that $\zeta_p \in K_h$ if and only if

$$-h \equiv \frac{q^f - 1}{q^{f_p} - 1} \pmod{e_p}. \tag{5.24}$$

To determine whether ζ_p is in K_h^{ij} we recall that by Remark 4.3, $\boldsymbol{\mu}$ is the restriction of $\boldsymbol{\sigma}^{e_0/b}$ to K_h and $\boldsymbol{\nu}$ is the restriction of $\boldsymbol{\sigma}^{v_h}\boldsymbol{\tau}^{c_h}$ to K_h. It follows that $\boldsymbol{\gamma} = \boldsymbol{\mu}^i\boldsymbol{\nu}^j$ is the restriction to K_h of

$$(\boldsymbol{\sigma}^{e_0/b})^i(\boldsymbol{\sigma}^{v_h}\boldsymbol{\tau}^{c_h})^j = \boldsymbol{\sigma}^r\boldsymbol{\tau}^{c_h j}, \tag{5.25}$$

where

$$r = \frac{e_0 i}{b} + \frac{q^{c_h j} - 1}{q^{c_h} - 1} v_h. \tag{5.26}$$

Thus $\zeta_p \in K_h^{ij}$ if and only if $f_p \mid c_h j$ and

$$\frac{e_0 i}{b} + \frac{q^{c_h j} - 1}{q^{c_h} - 1} v_h \equiv \frac{q^{c_h j} - 1}{q^{f_p} - 1} \pmod{e_p}. \tag{5.27}$$

Using (5.6), (5.17), and (5.27) we get a formula for $\sum_{L \in \mathscr{E}(K_h,1,p)} |\mathrm{Aut}(L/F)|$ in the case $\zeta_p \in K_h$.

Proposition 5.5. *If $\zeta_p \in K_h$ then*

$$\begin{aligned}\sum_{L \in \mathscr{E}(K_h,1,p)} |\mathrm{Aut}(L/F)| = &-\frac{p^2 bf}{c_h} + (p^2+p) \sum_{i=0}^{b-1} \sum_{j=0}^{\frac{f}{c_h}-1} p^{\frac{n_F e_0 f}{o(h,i,j)}} \\ &+ (p^2-p) \sum_{\substack{0 \leqslant j < f/c_h \\ f_p \mid c_h j}} \sum_{i \in R_{h,j}} p^{\frac{n_F e_0 f}{o(h,i,j)}},\end{aligned} \tag{5.28}$$

where $R_{h,j}$ denotes the set of integers $0 \leqslant i < b$ satisfying congruence (5.27).

By combining Propositions 5.3 and 5.5 with Eq. (5.2), we get the main result of this section.

Theorem 5.6. *Let F be a finite extension of $\mathbb{Q}_p$, let f and e be positive integers such that $p \,||\, e$, and set $e_0 = e/p$. Then the number of F-isomorphism classes of extensions of F with residue class degree f and ramification index e is*

$$\mathfrak{I}(F,f,e) = \frac{1}{fe} \sum_{h=0}^{e_0-1} \left(-\frac{p^2 bf}{c_h} + \sum_{i=0}^{b-1} \sum_{j=0}^{\frac{f}{c_h}-1} (p^2 + \omega_{hij}) p^{\frac{n_F e_0 f}{o(h,i,j)}} \right), \tag{5.29}$$

where

(i) $q =$ *the cardinality of the residue field of* F,
(ii) $b = (e_0, q^f - 1)$,
(iii) $u \in \mathbb{Z}$ *satisfies* $e_0 u \equiv b \pmod{q^f - 1}$,
(iv) c_h *is the smallest positive integer such that* $b \mid (q^{c_h} - 1)h$,
(v) $t(h,i,j) = \frac{q^{\mathrm{lcm}(f, c_h j)} - 1}{q^{c_h j} - 1} i + \frac{uhc_h j}{(f, c_h j)}$,
(vi) $o(h,i,j) = \frac{f}{(f, c_h j)} \cdot \frac{b}{(b, t(h,i,j))}$,
(vii)
$$\omega_{hij} = \begin{cases} p^2 & \text{if } e(F(\zeta_p)/F) \mid e,\ f(F(\zeta_p)/F) \mid f,\ f(F(\zeta_p)/F) \mid c_h j, \\ & \text{and } h,i,j \text{ satisfy (5.27)}, \\ p & \text{otherwise.} \end{cases}$$

6. The case $p^2 \,||\, e$

For the remainder of the paper we consider the case $p^2 \,||\, e$. Let $f_1 = f(F/\mathbb{Q}_p)$ and $e_1 = e(F/\mathbb{Q}_p)$, and write $e = p^2 e_0$ with $p \nmid e_0$. We make the following simplifying assumptions:

$$(p^{f_1 f} - 1, e_0) = 1,$$

$$f(F(\zeta_p)/F) \nmid f \quad \text{or} \quad e(F(\zeta_p)/F) > 1. \tag{6.1}$$

Some consequences of these assumptions are given in the following proposition.

Proposition 6.1. *Assume the conditions in* (6.1), *and let* $K \in \mathscr{E}(F, f, e)$. *Then*:
(i) *There is a unique field* L_K *such that* $F \subset L_K \subset K$ *and* K/L_K *is totally ramified of degree* p^2.
(ii) *There is a unique field* E_K *such that* $F \subset E_K \subset K$ *and* E_K/F *is totally ramified of degree* e_0.
(iii) E_K *is a subfield of* L_K.
(iv) $\mathrm{Aut}(K/F)$ *acts trivially on* E_K.
(v) $\zeta_p \notin K$.

Proof. Conditions (i)–(iv) follow from Proposition 3.2. To prove (v), note that $e(F(\zeta_p)/F) \mid (p-1)$ and $(p-1, e) = 1$. Thus if $e(F(\zeta_p)/F) > 1$ then $e(F(\zeta_p)/F) \nmid e$. Since $\zeta_p \in K$ implies $e(F(\zeta_p)/F) \mid e$ and $f(F(\zeta_p)/F) \mid f$, we must have $\zeta_p \notin K$. □

The approach we take here is somewhat different from that of Sections 4 and 5. Even with the conditions in (6.1), the computations that we will face are quite lengthy. To control the overall length of the paper and maintain readability, we will

describe the reasoning behind our computations but omit the details. All the computations in these section have been checked using *Mathematica* [22].

For each positive integer d, let

$$\mathscr{B}_d = \{K \in \mathscr{E}(F,f,e) : d \mid |\mathrm{Aut}(K/F)|\}. \tag{6.2}$$

Using (1.3) and the fact that $\sum_{d|n} \phi(d) = n$ we get

$$\mathfrak{I}(F,f,e) = \frac{1}{fe} \sum_{d>0} \phi(d)|\mathscr{B}_d|, \tag{6.3}$$

where ϕ is the Euler function. For $d>0$ and $i = 0,1,2$, put

$$\mathscr{C}_d^i = \{K \in \mathscr{B}_d : \exists F \subset N \subset K \text{ such that } K/N \text{ is Galois,}$$
$$e(K/N) = p^i, \text{ and } d \mid [K:N]\}. \tag{6.4}$$

By Proposition 6.1(iv) we have $\mathscr{B}_d = \mathscr{C}_d^2 \cup \mathscr{C}_d^1 \cup \mathscr{C}_d^0$. Therefore

$$|\mathscr{B}_d| = |\mathscr{C}_d^2| + |\mathscr{C}_d^1 \backslash \mathscr{C}_d^2| + |\mathscr{C}_d^0 \backslash (\mathscr{C}_d^1 \cup \mathscr{C}_d^2)|. \tag{6.5}$$

More precisely, $\mathscr{C}_d^2$ consists of the fields $K \in \mathscr{B}_d$ such that the ramification index of K over the fixed field of $\mathrm{Aut}(K/F)$ is p^2; $\mathscr{C}_d^1 \backslash \mathscr{C}_d^2$ consists of the fields $K \in \mathscr{B}_d$ such that the ramification index of K over the fixed field of $\mathrm{Aut}(K/F)$ is p; and $\mathscr{C}_d^0 \backslash (\mathscr{C}_d^1 \cup \mathscr{C}_d^2)$ consists of the fields $K \in \mathscr{B}_d$ such that the ramification index of K over the fixed field of $\mathrm{Aut}(K/F)$ is 1.

We will determine $|\mathscr{C}_d^2|$, $|\mathscr{C}_d^1 \backslash \mathscr{C}_d^2|$, and $|\mathscr{C}_d^0 \backslash (\mathscr{C}_d^1 \cup \mathscr{C}_d^2)|$ separately in Sections 7–9. In our computations, we will frequently encounter a tower of finite extensions $\mathbb{Q}_p \subset T \subset L \subset K$, where K/T is Galois, L/T is unramified of degree d, K/L is abelian of degree p^i, and $\zeta_p \notin L$. We need to give an explicit description of $\mathrm{Gal}(K/T)$ in terms of $\mathrm{Gal}(K/L)$.

Let L/T be an unramified extension of degree d and define

$$\mathfrak{R}(T,L;p^i) = \{K : L \subset K \subset \Omega,\ K/L \text{ abelian of degree } p^i,\ K/T \text{ Galois}\}. \tag{6.6}$$

For positive integers m and n, put

$$C(m) = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \end{bmatrix}_{m \times m}, \tag{6.7}$$

$$D(m,n)=\left.\begin{bmatrix} C(m) & 0_{m\times m} & \dots & 0_{m\times m} \\ 0_{m\times m} & C(m) & \dots & 0_{m\times m} \\ \vdots & \vdots & \ddots & \vdots \\ 0_{m\times m} & 0_{m\times m} & \dots & C(m) \end{bmatrix}\right\} n, \tag{6.8}$$

$$E(m,n)=\begin{bmatrix} 1 & 0_{1\times mn} \\ 0_{mn\times 1} & D(m,n) \end{bmatrix}. \tag{6.9}$$

We have an isomorphism of groups

$$L^\times/(L^\times)^{p^i}\cong\frac{\langle\pi_L\rangle}{\langle\pi_L^{p^i}\rangle}\times\frac{1+\pi_L\mathcal{O}_L}{(1+\pi_L\mathcal{O}_L)^{p^i}}\cong(\mathbb{Z}/p^i\mathbb{Z})^{1+n_L}. \tag{6.10}$$

Let $\boldsymbol{\sigma}$ be the Frobenius map of L/T. Then by Proposition 3.3(i), there is a $(\mathbb{Z}/p^i\mathbb{Z})$-basis $\mathscr{S}$ for $L^\times/(L^\times)^{p^i}\cong(\mathbb{Z}/p^i\mathbb{Z})^{1+n_L}$ such that the matrix of $\boldsymbol{\sigma}$ with respect to $\mathscr{S}$ is $E(d,n_T)$.

Define $\mathscr{H}(m,n;p^i)$ to be the set of all $E(m,n)$-invariant subgroups of $(\mathbb{Z}/p^i\mathbb{Z})^{1+mn}$ of index p^i. By class field theory, there is a bijection between the set of all $\boldsymbol{\sigma}$-invariant subgroups of $L^\times/(L^\times)^{p^i}$ of index p^i and $\mathfrak{R}(T,L;p^i)$. This bijection induces a bijection between $\mathscr{H}(d,n_T;p^i)$ and $\mathfrak{R}(T,L;p^i)$, which is denoted by $H\mapsto K_H$. Furthermore, $\mathrm{Gal}(K_H/L)\cong(\mathbb{Z}/p^i\mathbb{Z})^{1+n_L}/H$ for each $H\in\mathscr{H}(d,n_T;p^i)$. For each $u\in(\mathbb{Z}/p^i\mathbb{Z})^{1+n_L}/H$ let $\boldsymbol{\omega}(u)$ be the element of $\mathrm{Gal}(K_H/L)$ which corresponds to u under this isomorphism.

Let M/T be the maximal unramified subextension of K_H/T. Since $\boldsymbol{\sigma}$ is the Frobenius of L/T, it can be extended to the Frobenius $\boldsymbol{\sigma}'$ of M/T. Let $\boldsymbol{\theta}$ be an arbitrary extension of $\boldsymbol{\sigma}'$ to an element of $\mathrm{Gal}(K_H/T)$. Then $\mathrm{Gal}(K_H/T)$ is generated by $\mathrm{Gal}(K_H/L)\cong(\mathbb{Z}/p^i\mathbb{Z})^{1+n_L}/H$ and $\boldsymbol{\theta}$, where

$$\boldsymbol{\theta}\boldsymbol{\omega}(u)\boldsymbol{\theta}^{-1}=\boldsymbol{\omega}(u^{\boldsymbol{\sigma}})=\boldsymbol{\omega}(E(d,n_T)u) \tag{6.11}$$

for all $u\in(\mathbb{Z}/p^i\mathbb{Z})^{1+n_L}/H$, and $\boldsymbol{\theta}^d=\boldsymbol{\omega}\left(\begin{bmatrix}a\\ \alpha\end{bmatrix}\right)$ for some $a\in\mathbb{Z}/p^i\mathbb{Z}\cong\langle\pi_L\rangle/\langle\pi_L^{p^i}\rangle$ and $\alpha\in(\mathbb{Z}/p^i\mathbb{Z})^{n_L}\cong(1+\pi_L\mathcal{O}_L)/(1+\pi_L\mathcal{O}_L)^{p^i}$. It follows from the definition of $\boldsymbol{\theta}$ that the restriction of $\boldsymbol{\theta}^d$ to M/L is the Frobenius. By class field theory this implies $a\equiv 1\pmod{p^i}$.

To summarize, we have the following description of the structure of $\mathrm{Gal}(K_H/T)$.

Proposition 6.2. *Let $\mathbb{Q}_p\subset T\subset L$ be finite extensions such that L/T is unramified of degree d and $\zeta_p\notin L$. Let $H\mapsto K_H$ be the bijection between $\mathscr{H}(d,n_T;p^i)$ and $\mathfrak{R}(T,L;p^i)$ induced by class field theory. Then for each $H\in\mathscr{H}(d,n_T;p^i)$ we have an isomorphism $\boldsymbol{\omega}:(\mathbb{Z}/p^i\mathbb{Z})^{1+n_L}/H\to\mathrm{Gal}(K_H/L)$ such that $\mathrm{Gal}(K_H/T)$ is generated by $\mathrm{Gal}(K_H/L)$*

and an element $\boldsymbol{\theta}$ *satisfying*

$$\boldsymbol{\theta}^d = \boldsymbol{\omega}\left(\begin{bmatrix}1\\ \alpha\end{bmatrix}\right),$$

$$\boldsymbol{\theta}\boldsymbol{\omega}(u)\boldsymbol{\theta}^{-1} = \boldsymbol{\omega}(E(d,n_T)u) \quad \textit{for all } u\in(\mathbb{Z}/p^i\mathbb{Z})^{1+n_L}/H, \tag{6.12}$$

where $\begin{bmatrix}1\\ \alpha\end{bmatrix}\in(\mathbb{Z}/p^i\mathbb{Z})^{n_L+1}/H$ *depends only on* T *and* L.

Next, we list the elements H of $\mathscr{H}(d,n_T;p^i)$ for $i=1,2$. For each such H we will give a more explicit description of the structure of $\mathrm{Gal}(K_H/T)$ than that given in Proposition 6.2. These explicit descriptions will be essential in our later calculations.

Corollary 6.3. *Let* $\mathbb{Q}_p\subset T\subset L\subset\Omega$ *be as in Proposition* 6.2. *Then the elements of* $\mathscr{H}(d,n_T;p)$ *are the groups of the form*

$$H(\lambda,a) = a^{\perp} = \{x\in(\mathbb{Z}/p\mathbb{Z})^{1+n_L} : x^t a = 0\}, \tag{6.13}$$

where $0\neq a\in(\mathbb{Z}/p\mathbb{Z})^{1+n_L}$ *satisfies* $E(d,n_T)^t a = \lambda a$ *for some* $\lambda\in\mathbb{Z}/p\mathbb{Z}$ *such that* $\lambda^d = 1$. *Furthermore,* $\mathrm{Gal}(K_{H(\lambda,a)}/T)$ *is generated by*

$$\mathrm{Gal}(K_{H(\lambda,a)}/L) = \langle\boldsymbol{\kappa}\rangle\cong\mathbb{Z}/p\mathbb{Z} \tag{6.14}$$

and an element $\boldsymbol{\theta}$ *such that* $\boldsymbol{\theta}^d = \boldsymbol{\kappa}^{c(a)}$ *and* $\boldsymbol{\theta}\boldsymbol{\kappa}\boldsymbol{\theta}^{-1} = \boldsymbol{\kappa}^{\lambda}$, *where* $c(a) = \begin{bmatrix}1\\ \alpha\end{bmatrix}^t a\in\mathbb{Z}/p\mathbb{Z}$ *for some fixed* $\alpha\in(\mathbb{Z}/p\mathbb{Z})^{n_L}$.

We omit the proof of Corollary 6.3 since it is a simpler version of the proof of the next corollary.

Corollary 6.4. *Let* $\mathbb{Q}_p\subset T\subset L\subset\Omega$ *be as in Proposition* 6.2, *and let* H *be a subgroup of* $(\mathbb{Z}/p^2\mathbb{Z})^{1+n_L}$ *of index* p^2.

(i) *If* $(\mathbb{Z}/p^2\mathbb{Z})^{1+n_L}/H\cong\mathbb{Z}/p^2\mathbb{Z}$, *then* $H\in\mathscr{H}(d,n_T;p^2)$ *if and only if* H *is of the form*

$$H(\lambda,a) = a^{\perp} = \{x\in(\mathbb{Z}/p^2\mathbb{Z})^{1+n_L} : x^t a = 0\}, \tag{6.15}$$

where $\lambda\in\mathbb{Z}/p^2\mathbb{Z}$ *satisfies* $\lambda^d = 1$ *and* $a\in(\mathbb{Z}/p^2\mathbb{Z})^{1+n_L}\backslash(p\mathbb{Z}/p^2\mathbb{Z})^{1+n_L}$ *satisfies* $E(d,n_T)^t a = \lambda a$. *Furthermore,* $\mathrm{Gal}(K_{H(\lambda,a)}/T)$ *is generated by*

$$\mathrm{Gal}(K_{H(\lambda,a)}/L) = \langle\boldsymbol{\kappa}\rangle\cong\mathbb{Z}/p^2\mathbb{Z} \tag{6.16}$$

and an element $\boldsymbol{\theta}$ *such that* $\boldsymbol{\theta}^d = \boldsymbol{\kappa}^{c(a)}$ *and* $\boldsymbol{\theta}\boldsymbol{\kappa}\boldsymbol{\theta}^{-1} = \boldsymbol{\kappa}^{\lambda}$, *where* $c(a) = \binom{1}{\alpha}^t a \in \mathbb{Z}/p^2\mathbb{Z}$ *for some fixed* $\alpha \in (\mathbb{Z}/p^2\mathbb{Z})^{n_L}$.

(ii) *If* $(\mathbb{Z}/p^2\mathbb{Z})^{1+n_L}/H \cong (\mathbb{Z}/p\mathbb{Z})^2$, *then* $H \supset (p\mathbb{Z}/p^2\mathbb{Z})^{1+n_L}$. *In this case* $H \in \mathscr{H}(d, n_T; p^2)$ *if and only if* $(H/(p\mathbb{Z}/p^2\mathbb{Z})^{1+n_L})^{\perp}$ *is the column space of some* $(1+n_L)\times 2$ *matrix* A *over* $\mathbb{Z}/p\mathbb{Z}$ *such that* $\operatorname{rank}(A) = 2$ *and* $E(d, n_T)^t A = A\Lambda$ *for some* $\Lambda \in \mathrm{GL}(2,p)$ *satisfying* $\Lambda^d = I_2$. *Equivalently*, $H \in \mathscr{H}(d, n_T; p^2)$ *if and only of* H *is of the form*

$$H(\Lambda, A) = \{x \in (\mathbb{Z}/p^2\mathbb{Z})^{1+n_L} : x^t A \equiv 0 \pmod p\}, \tag{6.17}$$

where A *and* Λ *are as above. Furthermore*, $\mathrm{Gal}(K_{H(\Lambda,A)}/T)$ *is generated by*

$$\mathrm{Gal}(K_{H(\Lambda,A)}/L) = \langle \boldsymbol{\kappa}_1, \boldsymbol{\kappa}_2 \rangle \cong (\mathbb{Z}/p\mathbb{Z})^2 \tag{6.18}$$

and an element $\boldsymbol{\theta}$ *such that* $\boldsymbol{\theta}^d = \boldsymbol{\kappa}_1^{c_1(A)}\boldsymbol{\kappa}_2^{c_2(A)}$, $\boldsymbol{\theta}\boldsymbol{\kappa}_1\boldsymbol{\theta}^{-1} = \boldsymbol{\kappa}_1^{\lambda_{11}}\boldsymbol{\kappa}_2^{\lambda_{12}}$, *and* $\boldsymbol{\theta}\boldsymbol{\kappa}_2\boldsymbol{\theta}^{-1} = \boldsymbol{\kappa}_1^{\lambda_{21}}\boldsymbol{\kappa}_2^{\lambda_{22}}$, *where* $(c_1(A), c_2(A)) = \binom{1}{\alpha}^t A \in (\mathbb{Z}/p\mathbb{Z})^2$ *for some fixed* $\alpha \in (\mathbb{Z}/p\mathbb{Z})^{n_L}$ *and* $[\lambda_{ij}] = \Lambda$.

Proof. In both cases the necessary and sufficient conditions for H to be an element of $\mathscr{H}(d, n_T; p^2)$ are straightforward from the definitions. It remains to show that for $H \in \mathscr{H}(d, n_T; p^2)$, the structure of $\mathrm{Gal}(K_H/T)$ is as described. We will only give the argument for case (i), as case (ii) is quite similar.

By Proposition 6.2, $\mathrm{Gal}(K_H/T)$ is generated by $\mathrm{Gal}(K_H/L) \cong (\mathbb{Z}/p^2\mathbb{Z})^{1+n_L}/H$ and an element $\boldsymbol{\theta}$ satisfying relations (6.12). We have $H = H(\lambda, a) = a^{\perp}$ for some $\lambda \in \mathbb{Z}/p^2\mathbb{Z}$ and $a \in (\mathbb{Z}/p^2\mathbb{Z})^{n_L} \backslash (p\mathbb{Z}/p^2\mathbb{Z})^{n_L}$ such that $E(d, n_T)^t a = \lambda a$ and $\lambda^d = 1$. There is a canonical isomorphism

$$\begin{array}{ccc} \psi : (\mathbb{Z}/p^2\mathbb{Z})^{n_L+1}/a^{\perp} & \to & \mathrm{Hom}_{\mathbb{Z}/p^2\mathbb{Z}}(\langle a \rangle, \mathbb{Z}/p^2\mathbb{Z}), \\ x + a^{\perp} & \mapsto & \langle \cdot, x \rangle, \end{array} \tag{6.19}$$

where $\langle \cdot, \cdot \rangle$ is the standard inner product on $(\mathbb{Z}/p^2\mathbb{Z})^{n_L}$. It follows that the conjugation action of $\boldsymbol{\theta}$ on $\mathrm{Gal}(K_H/L)$ induces an action of $\boldsymbol{\theta}$ on $\mathrm{Hom}_{\mathbb{Z}/p^2\mathbb{Z}}(\langle a \rangle, \mathbb{Z}/p^2\mathbb{Z})$. Let ϕ be the unique element of $\mathrm{Hom}(\langle a \rangle, \mathbb{Z}/p^2\mathbb{Z})$ such that $\phi(a) = 1$. Then $\psi\left(\binom{1}{\alpha}\right) = \left(\binom{1}{\alpha}^t a\right)\phi$ and $\boldsymbol{\theta} \cdot \phi = \lambda\phi$ for all $u \in \mathbb{Z}/p^2\mathbb{Z}$. Therefore, by identifying $\mathrm{Gal}(K_H/L)$ with $\mathrm{Hom}_{\mathbb{Z}/p^2\mathbb{Z}}(\langle a \rangle, \mathbb{Z}/p^2\mathbb{Z})$ using ψ and identifying $\mathrm{Hom}_{\mathbb{Z}/p^2\mathbb{Z}}(\langle a \rangle, \mathbb{Z}/p^2\mathbb{Z})$ with $\mathbb{Z}/p^2\mathbb{Z}$ using the basis $\{\phi\}$, we see that $\mathrm{Gal}(K_H/T)$ is

generated by $\mathrm{Gal}(K_H/L) = \langle \boldsymbol{\kappa} \rangle \cong \mathbb{Z}/p^2\mathbb{Z}$ and an element $\boldsymbol{\theta}$ satisfying the relations $\boldsymbol{\theta}^d = \boldsymbol{\kappa}^{c(a)}$ and $\boldsymbol{\theta}\boldsymbol{\kappa}\boldsymbol{\theta}^{-1} = \boldsymbol{\kappa}^{\lambda}$ with $c(a) = \begin{bmatrix}1\\ \alpha\end{bmatrix}^t a$, as claimed. □

7. Determination of $|\mathscr{C}_d^2|$

The goal of this section is to determine $|\mathscr{C}_d^2|$. We retain the notation of Section 6. In addition, we set $n = n_F = f_1 e_1$. Observe that $|\mathscr{C}_d^2| = 0$ if $d \nmid p^2 f$. Also note that $\mathscr{C}_d^2 = \mathscr{C}_{d'}^2$ where $d' = \mathrm{lcm}(p^2, d)$. Thus we assume that $d \mid p^2 f$ and $p^2 \mid d$.

Let $\mathscr{X}$ be the set of all (T, L, K) in the diagram

$$\begin{array}{c} \Omega \\ | \\ K \\ \text{(ram)} \;\big|\; p^2 \\ L \\ \text{(un)} \;\big|\; \frac{d}{p^2} \\ T \\ \big|\; \begin{array}{l} f(T/F) = \frac{p^2 f}{d} \\ e(T/F) = e_0 \end{array} \\ F \end{array}$$

such that K/T is Galois. Using Proposition 6.1(i)–(iv), we see that $(T, L, K) \mapsto K$ gives a bijection between $\mathscr{X}$ and $\mathscr{C}_d^2$. Hence $|\mathscr{C}_d^2| = |\mathscr{X}|$. Meanwhile, $|\mathscr{X}|$ can be computed by counting the elements $(T, L, K) \in \mathscr{X}$ in the order T, L, K.

Fix $T \in \mathscr{E}\left(F, \frac{p^2 f}{d}, e_0\right)$, let L/T be unramified of degree d/p^2, and let M/L be unramified of degree p. Then we have

$$|\{K : (T, L, K) \in \mathscr{X}\}| = |\mathfrak{R}(T, L; p^2)| - |\mathfrak{R}(T, M; p)|. \tag{7.1}$$

Using Corollary 6.3, we find that

$$\begin{aligned} |\mathfrak{R}(T, M; p)| &= \left| \mathscr{H}\left(\frac{d}{p}, \frac{p^2 e_0 fn}{d}; p\right) \right| \\ &= (p-1, d)\frac{p^{\frac{1}{d}p^2 e_0 fn} - 1}{p-1} + p^{\frac{1}{d}p^2 e_0 fn}. \end{aligned} \tag{7.2}$$

Lemma 7.1. *We have*

$$|\mathfrak{R}(T,L;p^2)| = \begin{cases} \left.\begin{aligned} &\frac{1}{2}(p-1,d)^2\frac{(p^{\frac{1}{d}p^2e_0fn}-1)^2}{(p-1)^2} \\ &\quad +(p-1,d)\frac{p^{\frac{1}{d}p^2e_0fn}(p^{\frac{1}{d}p^2e_0fn}-1)}{p-1} \\ &\quad +p^{\frac{1}{d}2p^2e_0fn}+\frac{1}{2}(p^2-1,d)\frac{p^{\frac{1}{d}2p^2e_0fn}-1}{p^2-1} \end{aligned}\right\} & \text{if } p^3\nmid d, \\ \left.\begin{aligned} &\frac{1}{2}(p-1,d)^2\frac{(p^{\frac{1}{d}p^2e_0fn}-1)^2}{(p-1)^2} \\ &+2(p-1,d)\frac{p^{\frac{1}{d}p^2e_0fn}(p^{\frac{1}{d}p^2e_0fn}-1)}{p-1} \\ &+p^{\frac{1}{d}p^2e_0fn}(2p^{\frac{1}{d}p^2e_0fn}-1) \\ &+\frac{1}{2}(p^2-1,d)\frac{p^{\frac{1}{d}2p^2e_0fn}-1}{p^2-1} \end{aligned}\right\} & \text{if } p^3\mid d. \end{cases} \tag{7.3}$$

Proof. First, we have

$$|\mathfrak{R}(T,L;p^2)| = \left|\mathscr{H}\left(\frac{d}{p^2},\frac{p^2e_0fn}{d};p^2\right)\right| = |\mathscr{H}_1|+|\mathscr{H}_2|, \tag{7.4}$$

where $\mathscr{H}_1$ and $\mathscr{H}_2$ are the subsets of $\mathscr{H}\left(\frac{d}{p^2},\frac{1}{d}p^2e_0fn;p^2\right)$ corresponding to the two cases of Corollary 6.4. Put $E=E\left(\frac{d}{p^2},\frac{1}{d}p^2e_0fn\right)$. Then

$$\begin{aligned} \mathscr{H}_1 = \{&H(\lambda,a): a\in(\mathbb{Z}/p^2\mathbb{Z})^{1+e_0fn}\backslash(p\mathbb{Z}/p^2\mathbb{Z})^{1+e_0fn},\ \lambda\in\mathbb{Z}/p^2\mathbb{Z}, \\ &E^ta=\lambda a,\ \lambda^{d/p^2}=1\}, \end{aligned} \tag{7.5}$$

$$\begin{aligned} \mathscr{H}_2 = \{&H(\Lambda,A): A\in M_{(1+e_0fn)\times 2}(\mathbb{Z}/p\mathbb{Z}),\ \operatorname{rank}(A)=2,\ \Lambda\in\mathrm{GL}(2,p), \\ &E^tA=A\Lambda,\ \Lambda^{d/p^2}=I_2\}. \end{aligned} \tag{7.6}$$

Let $\lambda\in\mathbb{Z}/p^2\mathbb{Z}$ satisfy $\lambda^{d/p^2}=1$. Then

$$|\{H(\lambda,a)\in\mathscr{H}_1\}| = \frac{|\mathscr{A}_\lambda|}{p^2-p} \tag{7.7}$$

where

$$\mathscr{A}_\lambda = \{a \in (\mathbb{Z}/p^2\mathbb{Z})^{1+e_0 fn} \backslash (p\mathbb{Z}/p^2\mathbb{Z})^{1+e_0 fn} : E^t a = \lambda a\}. \tag{7.8}$$

Hence

$$|\mathscr{H}_1| = \sum_{\substack{\lambda \in \mathbb{Z}/p\mathbb{Z} \\ \lambda^{d/p^2}=1}} |\{H(\lambda, a) \in \mathscr{H}_1\}| = \frac{1}{p^2 - p} \sum_{\substack{\lambda \in \mathbb{Z}/p\mathbb{Z} \\ \lambda^{d/p^2}=1}} |\mathscr{A}_\lambda|. \tag{7.9}$$

The cardinality of $\mathscr{A}_\lambda$ can be easily determined:

$$|\mathscr{A}_\lambda| = \begin{cases} p^{2(1+\frac{1}{d}p^2 e_0 fn)} - p^{1+\frac{1}{d}p^2 e_0 fn} & \text{if } \lambda = 1, \\ p^{1+\frac{2}{d}p^2 e_0 fn} - p^{1+\frac{1}{d}p^2 e_0 fn} & \text{if } \lambda \equiv 1 \pmod p \text{ but } \lambda \neq 1, \\ p^{\frac{2}{d}p^2 e_0 fn} - p^{\frac{1}{d}p^2 e_0 fn} & \text{if } \lambda \not\equiv 1 \pmod p. \end{cases} \tag{7.10}$$

Combining (7.9) and (7.10), we find that

$$\begin{aligned} |\mathscr{H}_1| = {} & (p-1, d)\left(p, \frac{d}{p^2}\right)\frac{p^{\frac{1}{d}p^2 e_0 fn - 1}(p^{\frac{1}{d}p^2 e_0 fn} - 1)}{p-1} \\ & + \left(p, \frac{d}{p^2}\right)p^{\frac{1}{d}p^2 e_0 fn - 1}(p^{\frac{1}{d}p^2 e_0 fn} - 1) + p^{\frac{1}{d}2p^2 e_0 fn}. \end{aligned} \tag{7.11}$$

To compute $|\mathscr{H}_2|$, we first observe that for $H(\Lambda, A) \in \mathscr{H}_2$ and $Q \in \mathrm{GL}(2,p)$, we have

$$H(\Lambda, A) = H(Q^{-1}\Lambda Q, AQ). \tag{7.12}$$

Also note that for $\Lambda \in \mathrm{GL}(2,p)$ with $\Lambda^{d/p^2} = I$, we have $H(\Lambda, A_1) = H(\Lambda, A_2)$ if and only if $A_1 = A_2 Q$ for some Q in the centralizer $\mathrm{cent}(\Lambda)$ of Λ in $\mathrm{GL}(2,p)$. Thus for each $\Lambda \in \mathrm{GL}(2,p)$,

$$|\{H(\Lambda, A) \in \mathscr{H}_2\}| = \frac{|\mathscr{A}_\Lambda|}{|\mathrm{cent}(\Lambda)|}, \tag{7.13}$$

where

$$\mathscr{A}_\Lambda = \{A \in M_{(1+e_0 fn)\times 2}(\mathbb{Z}/p\mathbb{Z}) : \ \mathrm{rank}(A) = 2, \ E^t A = A\Lambda\}. \tag{7.14}$$

By (7.12) and (7.13), we have

$$|\mathscr{H}_2| = \sum_{\Lambda} \frac{|\mathscr{A}_\Lambda|}{|\mathrm{cent}(\Lambda)|}, \tag{7.15}$$

where Λ runs over the set of canonical forms in $M_{2\times 2}(\mathbb{Z}/p\mathbb{Z})$ with $\Lambda^{d/p^2} = I$. We can compute $|\mathrm{cent}(\Lambda)|$ using the formula in [6], and $|\mathscr{A}_\Lambda|$ using the well-known formula for the dimension of the solution set of $E^t A = A\Lambda$ [5, Theorem 4.4.14]. We omit the details of these computations and record the result for $|\mathscr{H}_2|$ below.

$$|\mathscr{H}_2| = \begin{cases} \left.\begin{aligned} &\frac{1}{2}(p-1,d)^2\frac{(p^{\frac{1}{d}p^2e_0fn}-1)^2}{(p-1)^2} \\ &\quad+(p-1,d)p^{-1+\frac{1}{d}p^2e_0fn}(p^{\frac{1}{d}p^2e_0fn}-1) \\ &\quad-(p^{\frac{1}{d}p^2e_0fn}-1)p^{-1+\frac{1}{d}p^2e_0fn} \\ &\quad+\frac{1}{2}(p^2-1,d)\frac{p^{\frac{1}{d}2p^2e_0fn}-1}{p^2-1} \end{aligned}\right\} & \text{if } p^3\nmid d, \\ \left.\begin{aligned} &\frac{1}{2}(p-1,d)^2\frac{(p^{\frac{1}{d}p^2e_0fn}-1)^2}{(p-1)^2} \\ &\quad+(p-1,d)\frac{p^{\frac{1}{d}p^2e_0fn}(p^{\frac{1}{d}p^2e_0fn}-1)}{p-1} \\ &\quad+\frac{1}{2}(p^2-1,d)\frac{p^{\frac{1}{d}2p^2e_0fn}-1}{p^2-1} \end{aligned}\right\} & \text{if } p^3\mid d. \end{cases} \tag{7.16}$$

Finally, (7.3) follows from (7.4), (7.11), and (7.16). □

We now state the main result of this section.

Proposition 7.2. *Let* $d' = \operatorname{lcm}(p^2, d)$. *Then we have*

$$|\mathscr{C}_d^2| = \begin{cases} 0 & \text{if } d\nmid p^2f, \\ e_0\left[\begin{aligned} &\frac{1}{2}(p-1,d)^2\frac{(p^{\frac{1}{d'}p^2e_0fn}-1)^2}{(p-1)^2} \\ &+(p-1,d)\frac{(p^{\frac{1}{d'}p^2e_0fn}-1)^2}{p-1} \\ &+p^{\frac{1}{d'}p^2e_0fn}(p^{\frac{1}{d'}p^2e_0fn}-1) \\ &+\frac{1}{2}(p^2-1,d)\frac{1}{p^2-1}(p^{\frac{1}{d'}2p^2e_0fn}-1)\end{aligned}\right] & \text{if } d\mid p^2f \text{ and } p^3\nmid d, \\ e_0\left[\begin{aligned} &\frac{1}{2}(p-1,d)^2\frac{(p^{\frac{1}{d'}p^2e_0fn}-1)^2}{(p-1)^2} \\ &+(p-1,d)\frac{(p^{\frac{1}{d'}p^2e_0fn}-1)(2p^{\frac{1}{d'}p^2e_0fn}-1)}{p-1} \\ &+2p^{\frac{1}{d'}p^2e_0fn}(p^{\frac{1}{d'}p^2e_0fn}-1) \\ &+\frac{1}{2}(p^2-1,d)\frac{p^{\frac{1}{d'}2p^2e_0fn}-1}{p^2-1}\end{aligned}\right] & \text{if } d\mid p^2f \text{ and } p^3\mid d. \end{cases}$$

Proof. By the comments at the beginning of the section it suffices to prove the proposition under the assumptions $d \mid p^2 f$ and $p^2 \mid d$. Using (7.1) we get

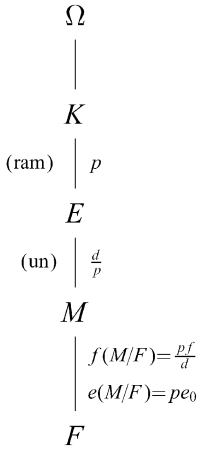
$$|\mathscr{C}_d^2| = |\mathscr{X}| = \sum_{T \in \mathscr{E}\left(F, \frac{1}{d}p^2 f, e_0\right)} (|\mathfrak{R}(T, L; p^2)| - |\mathfrak{R}(T, M; p)|). \tag{7.17}$$

The proposition now follows from (7.2), (7.3), and the fact that $\left|\mathscr{E}\left(F, \frac{1}{d}p^2 f, e_0\right)\right| = e_0$. □

8. Determination of $|\mathscr{C}_d^1 \backslash \mathscr{C}_d^2|$

In this section we compute the cardinality of $\mathscr{C}_d^1 \backslash \mathscr{C}_d^2$. Recall that $\mathscr{C}_d^1 \backslash \mathscr{C}_d^2$ consists of the fields $K \in \mathscr{E}(F, f, e)$ such that $d \mid |\mathrm{Aut}(K/F)|$ and the ramification index of K over the fixed field N_K of $\mathrm{Aut}(K/F)$ is p. Thus $|\mathscr{C}_d^1 \backslash \mathscr{C}_d^2| = 0$ if $d \nmid pf$. Furthermore, setting $d' = \mathrm{lcm}(p, d)$, we have $\mathscr{C}_d^1 \backslash \mathscr{C}_d^2 = \mathscr{C}_{d'}^1 \backslash \mathscr{C}_{d'}^2$. Therefore we may assume that $d \mid pf$ and $p \mid d$.

Let $\mathscr{X}$ be the set of all (M, E, K) in the diagram



such that K/M is Galois. The cardinality of $\mathscr{X}$ can be calculated by counting the elements $(M, E, K) \in \mathscr{X}$ in the order of M, E, K; when M and E are fixed, the number of K is $\left|\mathscr{H}\left(\frac{d}{p}, \frac{1}{d}p^2 e_0 fn; p\right)\right| - 1$, which is computed in (7.2). It turns out that

$$|\mathscr{X}| = pe_0(p^{1+\frac{1}{d}pe_0 fn} - p + 1)\left[(p-1, d)\frac{p^{\frac{1}{d}p^2 e_0 fn} - 1}{p-1} + p^{\frac{1}{d}p^2 e_0 fn} - 1\right]. \tag{8.1}$$

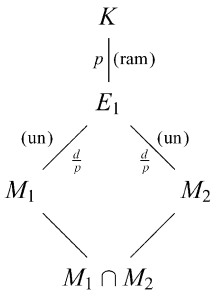
On the other hand, $\mathscr{X} = \mathscr{X}_1 \dot{\cup} \mathscr{X}_2$, where

$$\mathscr{X}_1 = \{(M, E, K) \in \mathscr{X} : K \in \mathscr{C}_d^1 \backslash \mathscr{C}_d^2\}, \tag{8.2}$$

$$\mathscr{X}_2 = \{(M, E, K) \in \mathscr{X} : K \in \mathscr{C}_d^1 \cap \mathscr{C}_d^2\}. \tag{8.3}$$

Lemma 8.1. *For each $K \in \mathscr{C}_d^1 \backslash \mathscr{C}_d^2$, there are unique subfields $M \subset E \subset K$ such that $(M, E, K) \in \mathscr{X}$.*

Proof. The existence of such an (M, E) follows from the definition of $\mathscr{C}_d^1$. To see the uniqueness of (M, E), we assume that there are (M_1, E_1) and (M_2, E_2) such that $(M_1, E_1, K) \in \mathscr{X}$ and $(M_2, E_2, K) \in \mathscr{X}$. Then $K/E_1 \cap E_2$ is totally ramified, and also Galois since both K/E_1 and K/E_2 are Galois. Therefore by Proposition 6.1, $[K : E_1 \cap E_2] \mid p^2$. If $E_1 \neq E_2$, we must have $[K : E_1 \cap E_2] = p^2$. However, this would imply that $K \in \mathscr{C}_d^2$, contrary to assumption. Thus $E_1 = E_2$. In the diagram

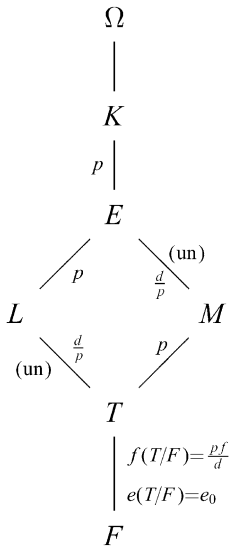


the extension $K/M_1 \cap M_2$ is Galois since both K/M_1 and K/M_2 are Galois. If $e(K/M_1 \cap M_2) > p$ then $e(K/M_1 \cap M_2) = p^2$, which implies $K \in \mathscr{C}_d^2$, contrary to assumption. Thus $E_1/M_1 \cap M_2$ is unramified, and hence $M_1 = M_2$. □

Lemma 8.1 implies that $(M, E, K) \mapsto K$ gives a bijection between $\mathscr{X}_1$ and $\mathscr{C}_d^1 \backslash \mathscr{C}_d^2$. Hence

$$|\mathscr{C}_d^1 \backslash \mathscr{C}_d^2| = |\mathscr{X}_1| = |\mathscr{X}| - |\mathscr{X}_2|. \tag{8.4}$$

In order to calculate $|\mathscr{X}_2|$, we let $\mathscr{Y}$ be the set of all (T, L, M, E, K) in the diagram



such that $T = L \cap M$ and K/T is Galois. Put

$$\mathscr{Z}_1 = \{(T, L, M, E, K) \in \mathscr{Y} : E/L \text{ is unramified}\}, \tag{8.5}$$

$$\mathscr{Z}_2 = \{(T, L, M, E, K) \in \mathscr{Y} : E/L \text{ is ramified but } K/E \text{ is unramified}\}. \tag{8.6}$$

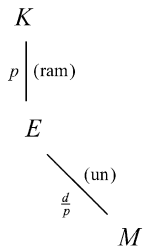
Lemma 8.2. *The map*

$$\begin{array}{rccc} \eta: & \mathscr{Y}\backslash(\mathscr{Z}_1 \cup \mathscr{Z}_2) & \to & \mathscr{X}_2 \\ & (T, L, M, E, K) & \mapsto & (M, E, K) \end{array} \tag{8.7}$$

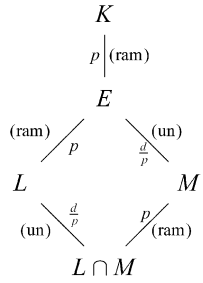
is a bijection.

Proof. For each $(T, L, M, E, K) \in \mathscr{Y}\backslash(\mathscr{Z}_1 \cup \mathscr{Z}_2)$, the extension K/L is totally ramified of degree p^2. By Proposition 6.1(i), L is uniquely determined by K. Consequently, $T = L \cap M$ is determined by K and M, so η is one-to-one.

On the other hand, for each $(M,E,K)\in\mathscr{X}_2$, we have a diagram



with K/M Galois. Let L/F be the unique subextension of K/F such that K/L is totally ramified of degree p^2. Since $K\in\mathscr{C}_d^2$, the extension K/L is Galois. Clearly, $L\subset E$, and in the diagram



the extension $K/L\cap M$ is Galois. Hence $(L\cap M,L,M,E,K)\in\mathscr{Y}\setminus(\mathscr{Z}_1\cup\mathscr{Z}_2)$. This proves that η is onto. $\square$

It follows from Lemma 8.2 that

$$|\mathscr{X}_2| = |\mathscr{Y}| - |\mathscr{Z}_1| - |\mathscr{Z}_2|. \tag{8.8}$$

The cardinality of $\mathscr{Z}_1$ can be calculated by counting the elements (T,L,M,E,K) in the order T,E,K,L,M. Fix T and E. Then the number of K is $\left|\mathscr{H}\left(d,\frac{1}{d}pe_0fn;p\right)\right|$, and the number of (L,M) is 0 if $(p,d/p)\neq 1$, and 1 if $(p,d/p)=1$. It follows that

$$|\mathscr{Z}_1| = \begin{cases} e_0\left[(p-1,d)\dfrac{p^{\frac{1}{d}pe_0fn}-1}{p-1}+p^{\frac{1}{d}pe_0fn}\right] & \text{if } p^2\nmid d,\\ 0 & \text{if } p^2\mid d. \end{cases} \tag{8.9}$$

Lemma 8.3. *We have*

$$|\mathscr{Y}| = \begin{cases} e_0\left[(p-1,d)^2\cdot\dfrac{p(p^{\frac{1}{d}pe_0fn}-1)^2}{(p-1)^2}+p^{\frac{1}{d}pe_0fn}\right. & \\ \left.\quad+(p-1,d)\dfrac{(p^{\frac{1}{d}pe_0fn}-1)(p^{1+\frac{1}{d}pe_0fn}+1)}{p-1}\right] & \text{if } p^2\nmid d, \\ e_0\left[(p-1,d)^2\cdot\dfrac{p(p^{\frac{1}{d}pe_0fn}-1)^2}{(p-1)^2}\right. & \\ \quad+2(p-1,d)\dfrac{p^{1+\frac{1}{d}pe_0fn}(p^{\frac{1}{d}pe_0fn}-1)}{p-1} & \\ \quad+p^{1+\frac{1}{d}pe_0fn}(p^{\frac{1}{d}pe_0fn}-1) & \\ \left.\quad-\dfrac{(p^{\frac{1}{d}pe_0fn}-1)(p^{\frac{1}{d}pe_0fn}-p)}{p^2-1}\right] & \text{if } p^2\mid d. \end{cases} \tag{8.10}$$

Proof. First fix $T\in\mathscr{E}\left(F,\frac{1}{d}pf,e_0\right)$ and let L/T be unramified of degree d/p. Put $\mathscr{H}=\mathscr{H}\left(\frac{d}{p},\frac{1}{d}pe_0fn;p^2\right)$, and let $H\mapsto K_H$ be the bijection between $\mathscr{H}$ and $\mathfrak{R}(T,L;p^2)$ induced by class field theory. For each $H\in\mathscr{H}$, the number of (M,E) such that $(T,L,M,E,K_H)\in\mathscr{Y}$ is equal to $|\mathscr{J}(H)|$, where

$$\mathscr{J}(H)=\{J\leqslant\mathrm{Gal}(K_H/T):|J|=d,\ \mathrm{Gal}(K_H/T)=\mathrm{Gal}(K_H/L)\cdot J\}. \tag{8.11}$$

Alternatively, $|\mathscr{J}(H)|$ is the number of subextensions M/T of K_H/T such that $[M:T]=p$ and $L\cap M=T$. For any such M, the compositum $E=LM$ is the only field such that $(T,L,M,E,K_H)\in\mathscr{Y}$. Therefore

$$|\{(M,E,K):(T,L,M,E,K)\in\mathscr{Y}\}|=\sum_{H\in\mathscr{H}}|\mathscr{J}(H)|. \tag{8.12}$$

For each $H\in\mathscr{H}$, the structure of $\mathrm{Gal}(K_H/T)$ and the position of $\mathrm{Gal}(K_H/L)$ in $\mathrm{Gal}(K_H/T)$ are explicitly described in Corollary 6.4. In fact, in the notation of Corollary 6.4(i),

$$\mathscr{J}(H(\lambda,a))=\{\langle\boldsymbol{\kappa}^p,\boldsymbol{\kappa}^c\boldsymbol{\theta}\rangle:c\in\mathbb{Z}/p^2\mathbb{Z},\ (\boldsymbol{\kappa}^c\boldsymbol{\theta})^{d/p}\in\langle\boldsymbol{\kappa}^p\rangle\}, \tag{8.13}$$

and $\langle \boldsymbol{\kappa}^p, \boldsymbol{\kappa}^c\boldsymbol{\theta}\rangle = \langle \boldsymbol{\kappa}^p, \boldsymbol{\kappa}^{c'}\boldsymbol{\theta}\rangle$ if and only if $c' - c \in p\mathbb{Z}/p^2\mathbb{Z}$. Therefore

$$\begin{aligned}
|\mathscr{J}(H(\lambda,a))| &= \frac{1}{p}|\{c\in\mathbb{Z}/p^2\mathbb{Z} : (\boldsymbol{\kappa}^c\boldsymbol{\theta})^{d/p}\in\langle\boldsymbol{\kappa}^p\rangle\}| \\
&= \frac{1}{p}\left|\left\{c\in\mathbb{Z}/p^2\mathbb{Z} : (1+\lambda+\cdots+\lambda^{\frac{d}{p}-1})c + \begin{bmatrix}1\\ \alpha\end{bmatrix}^t a \in p\mathbb{Z}/p^2\mathbb{Z}\right\}\right| \\
&= \begin{cases} p & \text{if } \lambda\neq 1, \\ 1 & \text{if } \lambda = 1,\ p^2\nmid d, \\ p & \text{if } \lambda = 1,\ p^2\mid d, \text{ and } \begin{bmatrix}1\\ \alpha\end{bmatrix}^t a\in p\mathbb{Z}/p^2\mathbb{Z}, \\ 0 & \text{if } \lambda = 1,\ p^2\mid d, \text{ and } \begin{bmatrix}1\\ \alpha\end{bmatrix}^t a\notin p\mathbb{Z}/p^2\mathbb{Z}. \end{cases}
\end{aligned} \tag{8.14}$$

Suppose instead we are in the situation of Corollary 6.4(ii). Then $H = H(\Lambda, A)$ for some Λ and A satisfying the conditions of the corollary. For each $J\in\mathscr{J}(H(\Lambda,A))$ the group $B = J\cap\langle\boldsymbol{\kappa}_1,\boldsymbol{\kappa}_2\rangle$ is a normal subgroup of J of order p, and $\boldsymbol{\kappa}_1^{c_1}\boldsymbol{\kappa}_2^{c_2}\boldsymbol{\theta}\in J$ for some $(c_1,c_2)\in(\mathbb{Z}/p\mathbb{Z})^2$. It follows that B is invariant under conjugation by $\boldsymbol{\theta}$, so $B = \langle\boldsymbol{\kappa}_1^{b_1}\boldsymbol{\kappa}_2^{b_2}\rangle$ with $\begin{bmatrix}b_1\\ b_2\end{bmatrix}$ an eigenvector of Λ^t. Therefore $J = \langle\boldsymbol{\kappa}_1^{b_1}\boldsymbol{\kappa}_2^{b_2}, \boldsymbol{\kappa}_1^{c_1}\boldsymbol{\kappa}_2^{c_2}\boldsymbol{\theta}\rangle$, with $(\boldsymbol{\kappa}_1^{c_1}\boldsymbol{\kappa}_2^{c_2}\boldsymbol{\theta})^{d/p}\in B$. Moreover, $\langle\boldsymbol{\kappa}_1^{b_1}\boldsymbol{\kappa}_2^{b_2}, \boldsymbol{\kappa}_1^{c_1}\boldsymbol{\kappa}_2^{c_2}\boldsymbol{\theta}\rangle = \langle\boldsymbol{\kappa}_1^{b_1}\boldsymbol{\kappa}_2^{b_2}, \boldsymbol{\kappa}_1^{c_1'}\boldsymbol{\kappa}_2^{c_2'}\boldsymbol{\theta}\rangle$ if and only if $\boldsymbol{\kappa}_1^{c_1'-c_1}\boldsymbol{\kappa}_2^{c_2'-c_2}\in B$. Hence

$$\begin{aligned}
|\mathscr{J}(H(\Lambda,A))| &= \frac{1}{p}|\{(W,(c_1,c_2)) : W \text{ is a 1-dimensional eigenspace of } \Lambda^t \\
&\qquad \text{and } (\boldsymbol{\kappa}_1^{c_1}\boldsymbol{\kappa}_2^{c_2}\boldsymbol{\theta})^{d/p}\in\langle\boldsymbol{\kappa}_1^{b_1}\boldsymbol{\kappa}_2^{b_2}\rangle\}| \\
&= \frac{1}{p}\left|\left\{(W,(c_1,c_2)) : W \text{ is a 1-dimensional eigenspace of } \Lambda^t \right.\right. \\
&\qquad \left.\left. \text{and } (c_1,c_2)(I_2+\Lambda+\cdots+\Lambda^{\frac{d}{p}-1}) + \begin{bmatrix}1\\ \alpha\end{bmatrix}^t A\in W\right\}\right|.
\end{aligned} \tag{8.15}$$

Thus $|\mathscr{J}(H(\Lambda,A))|$ can be determined from the canonical form of Λ. This allows us to compute $\sum_{H\in\mathscr{H}}|\mathscr{J}(H)|$; we omit the details. Since $\sum_{H\in\mathscr{H}}|\mathscr{J}(H)|$ is independent of the choice of (T,L), by (8.12) we have

$$|\mathscr{Y}| = \left|\mathscr{E}\left(F,\frac{pf}{d},e_0\right)\right|\cdot\sum_{H\in\mathscr{H}}|\mathscr{J}(H)|, \tag{8.16}$$

and the formula (8.10) for $|\mathscr{Y}|$ follows. □

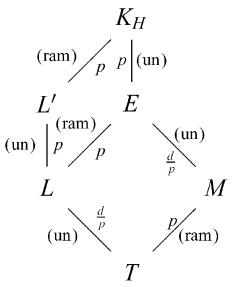
Lemma 8.4. *We have*

$$|\mathscr{Z}_2| = e_0(p-1,d)\frac{p(p^{\frac{1}{d}pe_0fn}-1)}{p-1}. \tag{8.17}$$

Proof. Fix $T \in \mathscr{E}\left(F, \frac{1}{d}pf, e_0\right)$, let L/T be unramified of degree d/p, and let L'/L be unramified of degree p. Let $H \mapsto K_H$ be the bijection between $\mathscr{H} = \mathscr{H}\left(d, \frac{1}{d}pe_0fn; p\right)$ and $\mathfrak{R}(T, L'; p)$ induced by class field theory. For each $H \in \mathscr{H}$, put

$$\mathscr{J}(H) = \{(B,J) : B \leqslant J \leqslant \mathrm{Gal}(K_H/T),\ |B| = p,\ |J| = d,$$
$$\text{and } \mathrm{Gal}(K_H/T) = \mathrm{Gal}(K_H/L') \cdot J\}. \tag{8.18}$$

When K_H/L' is ramified, the number of (M,E) such that $(T,L,M,E,K_H) \in \mathscr{Z}_2$ is equal to $|\mathscr{J}(H)|$. In the following diagram we have $T = L' \cap M$, and hence $\mathrm{Gal}(K_H/T) = \mathrm{Gal}(K_H/L') \cdot \mathrm{Gal}(K_H/M)$.



Therefore

$$|\{(M,E,K) : (T,L,M,E,K) \in \mathscr{Z}_2\}| = \sum_{\substack{H \in \mathscr{H} \\ K_H/L' \text{ ramified}}} |\mathscr{J}(H)|. \tag{8.19}$$

Corollary 6.3 allows us to compute $|\mathscr{J}(H)|$ for each $H \in \mathscr{H}$, and hence to compute (8.19). Omitting the details, we get

$$\sum_{\substack{H \in \mathscr{H} \\ K_H/L' \text{ ramified}}} |\mathscr{J}(H)| = (p-1,d)\frac{p(p^{\frac{1}{d}e_0fn}-1)}{p-1}. \tag{8.20}$$

Using (8.19) we see that $|\mathscr{Z}_2|$ is equal to (8.20) multiplied by the number of pairs (T,L), which is $\left|\mathscr{E}\left(F, \frac{1}{d}pf, e_0\right)\right| = e_0$. □

By (8.4) and (8.8) we have

$$|\mathscr{C}_d^1 \backslash \mathscr{C}_d^2| = |\mathscr{X}| - |\mathscr{Y}| + |\mathscr{Z}_1| + |\mathscr{Z}_2|, \tag{8.21}$$

where $|\mathscr{X}|$, $|\mathscr{Y}|$, $|\mathscr{Z}_1|$, and $|\mathscr{Z}_2|$ are given in (8.1), (8.10), (8.9), and (8.17). Hence we have a formula for $|\mathscr{C}_d^1 \backslash \mathscr{C}_d^2|$.

Proposition 8.5. *Let* $d' = \mathrm{lcm}(p, d)$. *Then we have*

$$|\mathscr{C}_d^1 \backslash \mathscr{C}_d^2| = \begin{cases} 0 & \text{if } d \nmid pf, \\ e_0\Big[-(p-1,d)^2 \dfrac{p}{(p-1)^2}(p^{\frac{1}{d'}pe_0 fn}-1)^2 & \\ \quad + (p-1,d)\dfrac{p}{p-1}(p^{\frac{1}{d'}p^2e_0 fn}-1 & \\ \quad + (p^{\frac{1}{d'}pe_0 fn}-1)(p^{1+\frac{1}{d'}p^2e_0 fn}-p^{\frac{1}{d'}pe_0 fn}-p+1)) & \\ \quad + p(p^{1+\frac{1}{d'}pe_0 fn}-p+1)(p^{\frac{1}{d'}p^2e_0 fn}-1)\Big] & \text{if } d \mid pf,\ p^2 \nmid d, \\ e_0\Big[-(p-1,d)^2 \dfrac{p}{(p-1)^2}(p^{\frac{1}{d'}pe_0 fn}-1)^2 & \\ \quad + (p-1,d)\dfrac{p}{p-1}(-(p^{\frac{1}{d'}pe_0 fn}-1)(2p^{\frac{1}{d'}pe_0 fn}-1) & \\ \quad + (p^{1+\frac{1}{d'}pe_0 fn}-p+1)(p^{\frac{1}{d'}p^2e_0 fn}-1)) & \\ \quad + p(p^{1+\frac{1}{d'}pe_0 fn}-p+1)(p^{\frac{1}{d'}p^2e_0 fn}-1) & \\ \quad - p^{1+\frac{1}{d'}pe_0 fn}(p^{\frac{1}{d'}pe_0 fn}-1) & \\ \quad + \dfrac{(p^{\frac{1}{d'}pe_0 fn}-1)(p^{\frac{1}{d'}pe_0 fn}-p)}{p^2-1}\Big] & \text{if } d \mid pf,\ p^2 \mid d. \end{cases}$$

9. Determination of $|\mathscr{C}_d^0 \backslash (\mathscr{C}_d^1 \cup \mathscr{C}_d^2)|$

Recall that $\mathscr{C}_d^0 \backslash (\mathscr{C}_d^1 \cup \mathscr{C}_d^2)$ consists of those fields $K \in \mathscr{E}(F, f, e)$ such that $d \mid |\mathrm{Aut}(K/F)|$ and the ramification index of K over the fixed field N_K of $\mathrm{Aut}(K/F)$ is 1. Thus $|\mathscr{C}_d^0 \backslash (\mathscr{C}_d^1 \cup \mathscr{C}_d^2)| = 0$ if $d \nmid f$, so we will assume that $d \mid f$.

Let $\mathscr{X}$ be the set of all (M, K) in the diagram

$$\begin{array}{c} \Omega \\ | \\ K \\ \text{(un)} \ | \ d \\ M \\ \Big| \begin{array}{l} f(M/F) = \frac{f}{d} \\ e(M/F) = p^2 e_0 \end{array} \\ F \end{array}$$

Then

$$|\mathscr{X}| = \left|\mathscr{E}\left(F, \frac{f}{d}, p^2 e_0\right)\right|$$
$$= e_0 p^2 (p^{2+\frac{1}{d}(p+1)e_0 fn} - p^{2+\frac{1}{d}pe_0 fn} + p^{1+\frac{1}{d}pe_0 fn} - p + 1). \tag{9.1}$$

On the other hand, $\mathscr{X} = \mathscr{X}_1 \dot\cup \mathscr{X}_2 \dot\cup \mathscr{X}_3$, where

$$\mathscr{X}_1 = \{(M,K) \in \mathscr{X} : K \in \mathscr{C}_d^0 \backslash (\mathscr{C}_d^1 \cup \mathscr{C}_d^2)\}, \tag{9.2}$$

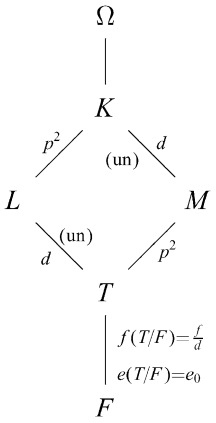
$$\mathscr{X}_2 = \{(M,K) \in \mathscr{X} : K \in \mathscr{C}_d^0 \cap (\mathscr{C}_d^1 \backslash \mathscr{C}_d^2)\}, \tag{9.3}$$

$$\mathscr{X}_3 = \{(M,K) \in \mathscr{X} : K \in \mathscr{C}_d^0 \cap \mathscr{C}_d^2\}. \tag{9.4}$$

For each $K \in \mathscr{C}_d^0 \backslash (\mathscr{C}_d^1 \cup \mathscr{C}_d^2)$, we claim that there is a unique M such that $(M,K) \in \mathscr{X}$. The existence of M follows from the definition of $\mathscr{C}_d^i$. To see the uniqueness of M, assume to the contrary that we have two different subextensions M_1/F and M_2/F of K/F such that K/M_1 and K/M_2 are both unramified of degree d. Then $K/M_1 \cap M_2$ is Galois and not unramified. By Proposition 6.1(iv), we must have $e(K/M_1 \cap M_2) = p$ or p^2. This means that $K \in \mathscr{C}_d^1 \cup \mathscr{C}_d^2$, which is a contradiction. It follows that

$$|\mathscr{C}_d^0 \backslash (\mathscr{C}_d^1 \cup \mathscr{C}_d^2)| = |\mathscr{X}_1| = |\mathscr{X}| - |\mathscr{X}_2| - |\mathscr{X}_3|. \tag{9.5}$$

We now determine $|\mathscr{X}_3|$. Let $\mathscr{Y}$ be the set of all (T, L, M, K) in the diagram



such that $T = L \cap M$ and K/T is Galois. Write $\mathscr{Y} = \mathscr{Y}_1 \dot\cup \mathscr{Y}_2$, where

$$\mathscr{Y}_1 = \{(T, L, M, K) \in \mathscr{Y} : e(K/L) = p^2\}, \tag{9.6}$$

$$\mathscr{Y}_2 = \{(T, L, M, K) \in \mathscr{Y} : e(K/L) = 1 \text{ or } p\}. \tag{9.7}$$

Then $(T, L, M, K) \mapsto (M, K)$ is a bijection between $\mathscr{Y}_1$ and $\mathscr{X}_3$ (cf. Proposition 6.1). Therefore

$$|\mathscr{X}_3| = |\mathscr{Y}_1| = |\mathscr{Y}| - |\mathscr{Y}_2|. \tag{9.8}$$

Lemma 9.1. *We have*

$$|\mathscr{Y}| = \begin{cases} e_0\left[\frac{1}{2}(p-1,d)^2\frac{p^2(p^{\frac{1}{d}e_0fn}-1)^2}{(p-1)^2}\right. & \\ \quad +(p-1,d)\frac{p(p^{\frac{1}{d}e_0fn}-1)}{p-1} & \\ \quad \left.+\frac{1}{2}(p^2-1,d)\frac{p^2(p^{\frac{1}{d}2e_0fn}-1)}{p^2-1}+1\right] & \text{if } p\nmid d, \\ e_0\left[\frac{1}{2}(p-1,d)^2\frac{p^2(p^{\frac{1}{d}e_0fn}-1)^2}{(p-1)^2}\right. & \\ \quad +(p-1,d)\frac{p^{2+\frac{1}{d}e_0fn}(p^{\frac{1}{d}e_0fn}-1)}{p-1} & \\ \quad \left.+\frac{1}{2}(p^2-1,d)\frac{p^2(p^{\frac{1}{d}2e_0fn}-1)}{p^2-1}\right] & \text{if } p\mid d. \end{cases} \tag{9.9}$$

Proof. The proof is similar to that of Lemma 8.3. Once again, we only describe the method and omit the computational details. Fix $T \in \mathscr{E}\left(F, \frac{f}{d}, e_0\right)$ and let L/T be the unramified extension of degree d. Let $H \mapsto K_H$ be the bijection between $\mathscr{H} = \mathscr{H}\left(d, \frac{1}{d}e_0 fn; p^2\right)$ and $\mathfrak{R}(T, L; p^2)$ induced by class field theory. For each $H \in \mathscr{H}$ we have

$$|\{M : (T, L, M, K_H) \in \mathscr{Y}\}| = |\mathscr{J}(H)|, \tag{9.10}$$

where

$$\mathscr{J}(H) = \{J \leqslant \mathrm{Gal}(K_H/T) : |J| = d,\ \mathrm{Gal}(K_H/T) = \mathrm{Gal}(K_H/L) \cdot J\}. \tag{9.11}$$

Using (9.10), we see that

$$|\{(M, K) : (T, L, M, K) \in \mathscr{Y}\}| = \sum_{H \in \mathscr{H}} |\mathscr{J}(H)|. \tag{9.12}$$

The sum $\sum_{H \in \mathscr{H}} |\mathscr{J}(H)|$ can be computed using Corollary 6.4, and the result is independent of the choice of (T, L) (cf. the proof of Lemma 8.3). Therefore we get $|\mathscr{Y}| = \left|\mathscr{E}\left(F, \frac{f}{d}, e_0\right)\right| \cdot \sum_{H \in \mathscr{H}} |\mathscr{J}(H)|$. □

Lemma 9.2. *We have*

$$|\mathscr{Y}_2| = \begin{cases} e_0\left[(p-1,d)\dfrac{p(p^{\frac{1}{d}e_0fn}-1)}{p-1}+1\right] & \text{if } p\nmid d, \\ 0 & \text{if } p\mid d. \end{cases} \tag{9.13}$$

Proof. By (9.7) we have $|\mathscr{Y}_2| = 0$ if $p \mid d$. Thus we may assume $p \nmid d$. Fix $T \in \mathscr{E}\left(F, \frac{f}{d}, e_0\right)$, let L/T be unramified of degree d, and let L'/L be unramified of degree p. Let $H \mapsto K_H$ be the bijection between $\mathscr{H} = \mathscr{H}\left(dp, \frac{1}{d}e_0 fn; p\right)$ and $\mathfrak{R}(T, L'; p)$ induced by class field theory. Then for each $H \in \mathscr{H}$ we have

$$|\{M : (T, L, M, K_H) \in \mathscr{Y}_2\}| = |\mathscr{J}(H)|, \tag{9.14}$$

where

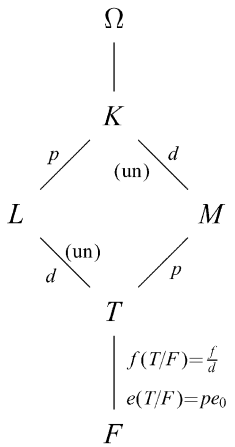
$$\mathscr{J}(H) = \{J \leqslant \mathrm{Gal}(K_H/T) : |J| = d\}. \tag{9.15}$$

It follows that

$$|\{(M, K) : (T, L, M, K) \in \mathscr{Y}_2\}| = \sum_{H \in \mathscr{H}} |\mathscr{J}(H)|, \tag{9.16}$$

which can be computed using Corollary 6.3. The lemma then follows from (9.16) and the formula $|\mathscr{Y}_2| = \left|\mathscr{E}\left(F, \frac{f}{d}, e_0\right)\right| \cdot \sum_{H \in \mathscr{H}} |\mathscr{J}(H)|$. □

Since $|\mathscr{X}_3|$ is determined by $|\mathscr{Y}|$ and $|\mathscr{Y}_2|$, the only part of (9.5) that remains to be computed is $|\mathscr{X}_2|$. Let $\mathscr{Z}$ be the set of all (T, L, M, K) in the diagram



such that $T = L \cap M$ and K/T is Galois. In addition, define

$$\mathscr{Z}_1 = \{(T, L, M, K) \in \mathscr{Z} : e(K/L) = p\}, \tag{9.17}$$

$$\mathscr{Z}_2 = \{(T, L, M, K) \in \mathscr{Z}_1 : K/L_K \text{ is Galois}\}, \tag{9.18}$$

where L_K is the unique field between F and K such that K/L_K is totally ramified of degree p^2. We claim that

$$\begin{array}{rccc} \psi: & \mathscr{Z}_1 \backslash \mathscr{Z}_2 & \to & \mathscr{X}_2 \\ & (T, L, M, K) & \mapsto & (M, K) \end{array} \tag{9.19}$$

is a bijection. By the definitions of $\mathscr{X}_2$, $\mathscr{Z}_1$, and $\mathscr{Z}_2$, it is clear that ψ is onto. Suppose that ψ is not one-to-one. Then there are elements (T_1, L_1, M, K) and (T_2, L_2, M, K) of $\mathscr{Z}_1 \backslash \mathscr{Z}_2$ such that $(T_1, L_1) \neq (T_2, L_2)$. Since $T_1 = L_1 \cap M$ and $T_2 = L_2 \cap M$, we must have $L_1 \neq L_2$. Since K/L_1 and K/L_2 are Galois and totally ramified of degree p, we see that $K/L_1 \cap L_2$ is Galois with $e(K/L_1 \cap L_2) > p$. Thus by Proposition 6.1(iv) we get $e(K/L_1 \cap L_2) = p^2$. This implies that $(T_1, L_1, M, K) \in \mathscr{Z}_2$, which is a contradiction. It follows that

$$|\mathscr{X}_2| = |\mathscr{Z}_1| - |\mathscr{Z}_2|. \tag{9.20}$$

Lemma 9.3. *We have*

$$|\mathscr{Z}_1| = e_0(p-1, d) \frac{p^2(p^{1+\frac{1}{d} e_0 fn} - p + 1)(p^{\frac{1}{d} pe_0 fn} - 1)}{p-1}. \tag{9.21}$$

Proof. Observe that

$$|\mathscr{Z}_1| = |\mathscr{Z}| - |\{(T, L, M, K) \in \mathscr{Z} : K/L \text{ unramified}\}|, \tag{9.22}$$

and that

$$\begin{aligned} |\{(T, L, M, K) \in \mathscr{Z} : K/L \text{ unram.}\}| &= \begin{cases} \left| \mathscr{E}\left(F, \frac{f}{d}, pe_0\right) \right| & \text{if } p \nmid d, \\ 0 & \text{if } p \mid d; \end{cases} \\ &= \begin{cases} pe_0(p^{1+\frac{1}{d} e_0 fn} - p + 1) & \text{if } p \nmid d, \\ 0 & \text{if } p \mid d. \end{cases} \end{aligned} \tag{9.23}$$

Meanwhile $|\mathscr{Z}|$ can be computed as before: Fix $T \in \mathscr{E}\left(F, \frac{f}{d}, pe_0\right)$ and let L/T be unramified of degree d. Let $H \mapsto K_H$ be the bijection between $\mathscr{H} = \mathscr{H}\left(d, \frac{1}{d} pe_0 fn; p\right)$

and $\mathfrak{R}(T,L;p)$ induced by class field theory. Then for each $H\in\mathscr{H}$ we have

$$|\{M:(T,L,M,K_H)\in\mathscr{Z}\}|=|\mathscr{J}(H)|, \tag{9.24}$$

where

$$\mathscr{J}(H)=\{J\leqslant \mathrm{Gal}(K_H/T):|J|=d,\ \mathrm{Gal}(K_H/T)=\mathrm{Gal}(K_H/L)\cdot J\}. \tag{9.25}$$

Consequently,

$$|\{(M,K):(T,L,M,K)\in\mathscr{Z}\}|=\sum_{H\in\mathscr{H}}|\mathscr{J}(H)|, \tag{9.26}$$

$$|\mathscr{Z}|=\left|\mathscr{E}\left(F,\frac{f}{d},pe_0\right)\right|\cdot\sum_{H\in\mathscr{H}}|\mathscr{J}(H)|. \tag{9.27}$$

Using (9.26) and Corollary 6.3 we get

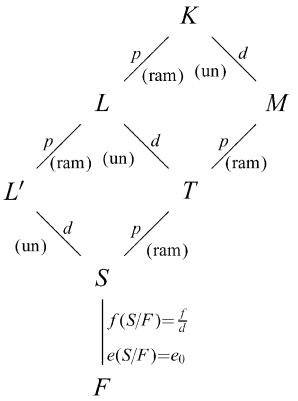
$$|\mathscr{Z}|=\begin{cases} e_0p(p^{1+\frac{1}{d}e_0fn}-p+1)\left[(p-1,d)\dfrac{p(p^{\frac{1}{d}pe_0fn}-1)}{p-1}+1\right] & \text{if } p\nmid d,\\[2ex] e_0(p-1,d)\dfrac{p^2(p^{1+\frac{1}{d}e_0fn}-p+1)(p^{\frac{1}{d}pe_0fn}-1)}{p-1} & \text{if } p\mid d. \end{cases} \tag{9.28}$$

Eq. (9.21) now follows from (9.22), (9.23), and (9.28). □

Lemma 9.4. *We have*

$$|\mathscr{Z}_2|=\begin{cases} e_0\left[\dfrac{1}{2}(p-1,d)^2\dfrac{p^2(p+1)(p^{\frac{1}{d}e_0fn}-1)^2}{(p-1)^2}\right.\\ \quad -(p-1,d)\dfrac{p^{2+\frac{1}{d}e_0fn}(p^{\frac{1}{d}e_0fn}-1)}{p-1}\\ \quad \left.+\dfrac{1}{2}(p^2-1,d)\dfrac{p^2(p^{\frac{1}{d}2e_0fn}-1)}{p-1}\right] & \text{if } p\nmid d,\\[2ex] e_0\left[\dfrac{1}{2}(p-1,d)^2\dfrac{p^2(p+1)(p^{\frac{1}{d}e_0fn}-1)^2}{(p-1)^2}\right.\\ \quad +(p-1,d)\dfrac{p^{2+\frac{1}{d}e_0fn}(p^{\frac{1}{d}e_0fn}-1)}{p-1}\\ \quad \left.+\dfrac{1}{2}(p^2-1,d)\dfrac{p^2(p^{\frac{1}{d}2e_0fn}-1)}{p-1}\right] & \text{if } p\mid d. \end{cases} \tag{9.29}$$

Proof. For each $(T, L, M, K) \in \mathscr{Z}_2$, we have a diagram



in which K/S is Galois, and S and L' are determined by (T, L, M, K). Thus if we let $\mathscr{W}$ denote the set of all (S, L', T, L, M, K) in this diagram such that K/S is Galois, we have $|\mathscr{Z}_2| = |\mathscr{W}|$. To compute $|\mathscr{W}|$, we fix $S \in \mathscr{E}\left(F, \frac{f}{d}, e_0\right)$ and let L'/S be unramified of degree d and N/L' unramified of degree p. Write $\mathfrak{K} = \mathfrak{K}(S, L'; p^2)$ and $\mathfrak{K}' = \{K \in \mathfrak{K} : N \subset K\} = \mathfrak{K}(S, N; p)$. For each $K \in \mathfrak{K}$, let

$$\mathscr{G}(K) = \{(B, J) : B \leqslant \mathrm{Gal}(K/L'),\ |B| = p,\ J \leqslant \mathrm{Gal}(K/S),$$
$$|J| = d,\ \mathrm{Gal}(K/S) = \mathrm{Gal}(K/L') \cdot J\}. \tag{9.30}$$

Note that if $(S, L', T, L, M, K) \in \mathscr{W}$, then $K \in \mathfrak{K} \backslash \mathfrak{K}'$. Also note that for each $K \in \mathfrak{K} \backslash \mathfrak{K}'$ we have

$$|\{(T, L, M) : (S, L', T, L, M, K) \in \mathscr{W}\}| = |\mathscr{G}(K)|. \tag{9.31}$$

More precisely, $(T, L, M) \leftrightarrow (\mathrm{Gal}(K/L), \mathrm{Gal}(K/M))$ is a bijection between the two sets in (9.31). Therefore

$$|\{(T, L, M, K) : (S, L', T, L, M, K) \in \mathscr{W}\}| = \sum_{K \in \mathfrak{K}} |\mathscr{G}(K)| - \sum_{K \in \mathfrak{K}'} |\mathscr{G}(K)|. \tag{9.32}$$

To compute $\sum_{K \in \mathfrak{K}} |\mathscr{G}(K)|$, let $H \mapsto K_H$ be the bijection between $\mathscr{H} = \mathscr{H}\left(d, \frac{1}{d} e_0 fn; p^2\right)$ and $\mathfrak{K}$ induced by class field theory, and let $\mathscr{H}_1$ and $\mathscr{H}_2$ be the subsets of $\mathscr{H}$ corresponding to the two cases of Corollary 6.4. We have $\mathrm{Gal}(K_H/L') \cong \mathbb{Z}/p^2\mathbb{Z}$ if $H \in \mathscr{H}_1$ and $\mathrm{Gal}(K_H/L') \cong (\mathbb{Z}/p\mathbb{Z})^2$ if $H \in \mathscr{H}_2$.

Therefore

$$|\mathscr{G}(K_H)| = \begin{cases} |\mathscr{J}(H)| & \text{if } H \in \mathscr{H}_1, \\ (p+1)|\mathscr{J}(H)| & \text{if } H \in \mathscr{H}_2, \end{cases} \tag{9.33}$$

where

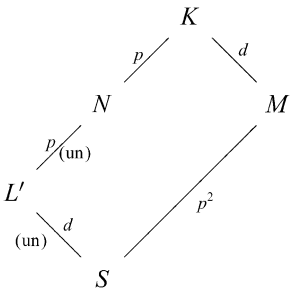
$$\mathscr{J}(H) = \{J \leqslant \mathrm{Gal}(K_H/S) : |J| = d,\ \mathrm{Gal}(K_H/S) = \mathrm{Gal}(K_H/L') \cdot J\}. \tag{9.34}$$

Thus

$$\sum_{K \in \mathfrak{K}} |\mathscr{G}(K)| = \sum_{H \in \mathscr{H}} |\mathscr{G}(K_H)| = \sum_{H \in \mathscr{H}_1} |\mathscr{J}(H)| + (p+1) \sum_{H \in \mathscr{H}_2} |\mathscr{J}(H)| \tag{9.35}$$

can be computed as before.

We now compute $\sum_{K \in \mathfrak{K}'} |\mathscr{G}(K)|$. We claim that if $p \mid d$, then $|\mathscr{G}(K)| = 0$ for all $K \in \mathfrak{K}'$. Suppose to the contrary that there exists $(B, J) \in \mathscr{G}(K)$ for some $K \in \mathfrak{K}'$. Let M denote the subfield of K fixed by J. Then we have the diagram



with $p \mid f(M/S)$. Thus $L' \cap M \neq S$, so $\mathrm{Gal}(K/S) \neq \mathrm{Gal}(K/L') \cdot J$, contrary to the definition of $\mathscr{G}(K)$. Therefore we may assume $p \nmid d$. Let $H \mapsto K_H$ be the bijection between $\mathscr{H}' = \mathscr{H}\left(dp, \frac{1}{d} e_0 fn; p\right)$ and $\mathfrak{K}'$ induced by class field theory. By Corollary 6.3, every $H \in \mathscr{H}'$ is of the form $H(\lambda, a) = a^{\perp}$ for some eigenvector a of $E\left(dp, \frac{1}{d} e_0 fn\right)^t$ with eigenvalue λ. Furthermore, $\mathrm{Gal}(K_{H(\lambda,a)}/S)$ is generated by $\mathrm{Gal}(K_{H(\lambda,a)}/N) = \langle \boldsymbol{\kappa} \rangle \cong \mathbb{Z}/p\mathbb{Z}$ and an element $\boldsymbol{\theta}$ such that $\boldsymbol{\theta}^{dp} = \boldsymbol{\kappa}^{c(a)}$ and $\boldsymbol{\theta}\boldsymbol{\kappa}\boldsymbol{\theta}^{-1} = \boldsymbol{\kappa}^{\lambda}$, where $c(a) = \left[\begin{smallmatrix} 1 \\ \alpha \end{smallmatrix}\right]^t a \in \mathbb{Z}/p\mathbb{Z}$ for some fixed $\alpha \in (\mathbb{Z}/p\mathbb{Z})^{pe_0 fn}$. Moreover, $\mathrm{Gal}(K_{H(\lambda,a)}/L')$ is generated by $\boldsymbol{\kappa}$ and $\boldsymbol{\theta}^d$ (cf. the proofs of Proposition 6.2 and Corollary 6.4). These explicit descriptions allow us to compute each $|\mathscr{G}(K_{H(\lambda,a)})|$, and hence to compute $\sum_{H \in \mathscr{H}'} |\mathscr{G}(K_H)| = \sum_{K \in \mathfrak{K}'} |\mathscr{G}(K)|$.

Now $|\{(T,L,M,K):(S,L',T,L,M,K)\in\mathscr{W}\}|$ can be computed using (9.32). After multiplying the result by $\left|\mathscr{E}\left(F,\frac{f}{d},e_0\right)\right|=e_0$, we get formula (9.29) for $|\mathscr{W}|=|\mathscr{Z}_2|$. $\square$

From (9.5), (9.8), and (9.20), we have

$$|\mathscr{C}_d^0\backslash(\mathscr{C}_d^1\cup\mathscr{C}_d^2)|=|\mathscr{X}|-|\mathscr{Z}_1|+|\mathscr{Z}_2|-|\mathscr{Y}|+|\mathscr{Y}_2|, \tag{9.36}$$

where $|\mathscr{X}|$, $|\mathscr{Y}|$, $|\mathscr{Y}_2|$, $|\mathscr{Z}_1|$, and $|\mathscr{Z}_2|$ are given in (9.1), (9.9), (9.13), (9.21), and (9.29). Thus we obtain the main result of this section.

Proposition 9.5. *We have*

$$|\mathscr{C}_d^0\backslash(\mathscr{C}_d^1\cup\mathscr{C}_d^2)|=\begin{cases}0 & \text{if } d\nmid f,\\ e_0p^2\left[\frac{1}{2}(p-1,d)^2\frac{p(p^{\frac{1}{d}e_0fn}-1)^2}{(p-1)^2}\right. & \\ \quad+\frac{1}{2}(p^2-1,d)\frac{p(p^{\frac{1}{d}2e_0fn}-1)}{p^2-1} & \\ \quad-\frac{(p-1,d)}{p-1}(p^{\frac{1}{d}e_0fn}(p^{\frac{1}{d}e_0fn}-1) & \\ \quad+(p^{1+\frac{1}{d}e_0fn}-p+1)(p^{\frac{1}{d}pe_0fn}-1)) & \\ \quad+p^{2+\frac{1}{d}(p+1)e_0fn}-p^{2+\frac{1}{d}pe_0fn} & \\ \quad\left.+p^{1+\frac{1}{d}pe_0fn}-p+1\right] & \text{if } d\mid f,\ p\nmid d,\\ e_0p^2\left[\frac{1}{2}(p-1,d)^2\frac{p(p^{\frac{1}{d}e_0fn}-1)^2}{(p-1)^2}\right. & \\ \quad+\frac{1}{2}(p^2-1,d)\frac{p(p^{\frac{1}{d}2e_0fn}-1)}{p^2-1} & \\ \quad-(p-1,d)\frac{(p^{\frac{1}{d}pe_0fn}-1)(p^{1+\frac{1}{d}e_0fn}-p+1)}{p-1} & \\ \quad+p^{2+\frac{1}{d}(p+1)e_0fn}-p^{2+\frac{1}{d}pe_0fn} & \\ \quad\left.+p^{1+\frac{1}{d}pe_0fn}-p+1\right] & \text{if } d\mid f,\ p\mid d.\end{cases}$$

10. Conclusion of the case $p^2 \,||\, e$

With $|\mathscr{C}_d^2|$, $|\mathscr{C}_d^1 \backslash \mathscr{C}_d^2|$, and $|\mathscr{C}_d^0 \backslash (\mathscr{C}_d^1 \cup \mathscr{C}_d^2)|$ computed in Sections 7–9, we are ready to state our main result in the case $p^2 \,||\, e$.

Theorem 10.1. *Let $F/\mathbb{Q}_p$ be a finite extension of degree n with residue degree f_1 and ramification index e_1. Let f, e, and e_0 be positive integers such that $e = p^2 e_0$, $p \nmid e_0$, $(p^{f_1 f} - 1, e_0) = 1$, and either $f(F(\zeta_p)/F) \nmid f$ or $e(F(\zeta_p)/F) > 1$. Write $f = p^i t$ with $p \nmid t$. Then the number of F-isomorphism classes of finite extensions K/F with residue degree f and ramification index e is given by*

$$
\begin{aligned}
\mathfrak{I}(F,f,e) = \frac{1}{p^i t} \sum_{\tau \mid t} \phi(\tau) \Bigg[& \frac{1}{2}(p-1,\tau)^2 \frac{(p^{\frac{t}{\tau} p^i e_0 n} - 1)^2}{p-1} \\
& - (p-1,\tau) \frac{p^{\frac{t}{\tau} p^i e_0 n}(p^{\frac{t}{\tau} p^i e_0 n} - 1)}{p-1} + \frac{1}{2}(p^2-1,\tau) \frac{(p^{\frac{t}{\tau} 2p^i e_0 n} - 1)}{p-1} \\
& + (p+1)(p^{1+\frac{t}{\tau}(p+1)p^i e_0 n} - p^{\frac{t}{\tau} p^i e_0 n}) - (p^2-1) p^{\frac{t}{\tau} p^{i+1} e_0 n} + p^{\frac{t}{\tau} 2p^i e_0 n} \\
& + \sum_{j=1}^{i} p^{j-1} \Bigg[\frac{(p^{\frac{t}{\tau} p^{i-j} e_0 n} - 1)(p^{\frac{t}{\tau} p^{i-j} e_0 n - 1} - 1)}{p+1} \\
& + (p-1)(-p^{2+\frac{t}{\tau} p^{i-j+1} e_0 n} + p^{\frac{t}{\tau} p^{i-j+1} e_0 n} + p^{\frac{t}{\tau} 2p^{i-j} e_0 n}) \\
& + (p^2-1)(p^{1+\frac{t}{\tau}(p+1)p^{i-j} e_0 n} - p^{\frac{t}{\tau} p^{i-j} e_0 n}) \\
& + \frac{1}{2}(p-1,\tau)^2 (p^{\frac{t}{\tau} p^{i-j} e_0 n} - 1)^2 + \frac{1}{2}(p^2-1,\tau)(p^{\frac{t}{\tau} 2p^{i-j} e_0 n} - 1) \Bigg] \Bigg].
\end{aligned}
$$

Proof. By (6.3) and (6.5) we have

$$
\mathfrak{I}(F,f,e) = \frac{1}{fe} \sum_{d>0} \phi(d)(n_0(d) + n_1(d) + n_2(d)), \tag{10.1}
$$

where $n_0(d) = |\mathscr{C}_d^0 \backslash (\mathscr{C}_d^1 \cup \mathscr{C}_d^2)|$, $n_1(d) = |\mathscr{C}_d^1 \backslash \mathscr{C}_d^2|$, and $n_2(d) = |\mathscr{C}_d^2|$. Since $n_2(d) = n_2(\mathrm{lcm}(p^2, d))$ and $n_2(d) = 0$ when $d \nmid p^2 f$, it follows that

$$
\sum_{d>0} \phi(d) n_2(d) = \sum_{d \mid p^{2+i} t} \phi(d) n_2(d)
$$

$$= \sum_{\tau|t} \phi(\tau)\left(\phi(1)n_2(\tau) + \phi(p)n_2(p\tau) + \phi(p^2)n_2(p^2\tau) + \sum_{j=3}^{2+i} \phi(p^j)n_2(p^j\tau)\right)$$

$$= \sum_{\tau|t} \phi(\tau)\left(p^2 n_2(p^2\tau) + (p-1)\sum_{j=3}^{2+i} p^{j-1} n_2(p^j\tau)\right). \quad (10.2)$$

By the same reasoning we have

$$\sum_{d>0} \phi(d)n_0(d) = \sum_{\tau|t} \phi(\tau)\left(n_0(\tau) + (p-1)\sum_{j=1}^{i} p^{j-1} n_0(p^j\tau)\right), \quad (10.3)$$

$$\sum_{d>0} \phi(d)n_1(d) = \sum_{\tau|t} \phi(\tau)\left(pn_1(p\tau) + (p-1)\sum_{j=2}^{1+i} p^{j-1} n_1(p^j\tau)\right). \quad (10.4)$$

It follows that

$$\mathfrak{I}(F,f,e) = \frac{1}{p^{2+i}te_0} \sum_{\tau|t} \phi(\tau)\left(n_0(\tau) + pn_1(p\tau) + p^2 n_2(p^2\tau) + (p-1)\sum_{j=1}^{i} p^{j-1}(n_0(p^j\tau) + pn_1(p^{j+1}\tau) + p^2 n_2(p^{j+2}\tau))\right). \quad (10.5)$$

Using Propositions 7.2, 8.5 and 9.5 to write out $n_0(p^j\tau) + pn_1(p^{j+1}\tau) + p^2 n_2(p^{j+2}\tau)$ explicitly for $0 \leqslant j \leqslant i$, we obtain the final formula for $\mathfrak{I}(F,f,e)$. □

References

[1] W.E. Clark, J.J. Liang, Enumeration of finite commutative chain rings, J. Algebra 27 (1973) 445–453.
[2] P. Deligne, Les corps locaux de caractéristique p, limites de corps locaux de caractéristique 0, in: Representations of Reductive Groups Over a Local Field, Hermann, Paris, 1984, pp. 119–157.
[3] I.B. Fesenko, S.V. Vostokov, Local Fields and their Extensions. A Constructive Approach, American Mathematical Society, Providence, RI, 1993.
[4] K.W. Gruenberg, A. Weiss, Galois invariants for local units, Quart. J. Math. Oxford 47 (1996) 25–39.
[5] R.A. Horn, C.R. Johnson, Topics in Matrix Analysis, Cambridge University Press, New York, 1991.
[6] X. Hou, $GL(m,2)$ acting on $R(r,m)/R(r-1,m)$, Discrete Math. 149 (1996) 99–122.
[7] X. Hou, q-ary bent functions constructed from chain rings, Finite Fields Appl. 4 (1998) 55–61.
[8] X. Hou, Bent functions, partial difference sets and quasi-Frobenius local rings, Des. Codes Cryptogr. 20 (2000) 251–268.
[9] X. Hou, Finite commutative chain rings, Finite Fields Appl. 7 (2001) 382–396.
[10] W. Klingenberg, Projective und affine Ebene mit Nachbarelementen, Math. Z. 60 (1960) 384–406.

[11] M. Krasner, Nombre des extensions d'un degré donné d'un corps p-adique: énoncé des résultats et préliminaires de la démonstration (espace des polynomes, transformation T), C. R. Acad. Sci. Paris 254 (1962) 3470–3472.
[12] M. Krasner, Nombre des extensions d'un degré donné d'un corps p-adique: suite de la démonstration, C. R. Acad. Sci. Paris 255 (1962) 224–226.
[13] M. Krasner, Nombre des extensions de degré donné d'un corps de nombre p-adique: les conditions d'Ore et la caractérisation de $E_{k,j}^{(n)}$; préliminaires du calcul de $N_{k,j,s}^{(n)}$, C. R. Acad. Sci. Paris 255 (1962) 1682–1684.
[14] M. Krasner, Nombre des extensions de degré donné d'un corps p-adique: calcul de $N_{k,j,s}^{(n)}$; démonstration du théorème 1, C. R. Acad. Sci. Paris 255 (1962) 2342–2344.
[15] M. Krasner, Nombre des extensions de degré donné d'un corps p-adique: compléments au théorème 1 dans le cas non p-adique; démonstration du théorème 2, C. R. Acad. Sci. Paris 255 (1962) 3095–3097.
[16] K.H. Leung, S.L. Ma, Constructions of partial difference sets and relative difference sets on p-groups, Bull. London Math. Soc. 22 (1990) 533–539.
[17] K.H. Leung, S.L. Ma, Partial difference sets with Paley parameters, Bull. London Math. Soc. 27 (1995) 553–564.
[18] B.R. McDonald, Finite Rings with Identity, Marcel Dekker, New York, 1974.
[19] J.-P. Serre, Local Fields, Springer, New York, 1979.
[20] G. Törner, F.D. Veldkamp, Literature on geometry over rings, J. Geom. 42 (1991) 180–200.
[21] A. Weiss, Multiplicative Galois Module Structure, American Mathematical Society, Providence, RI, 1996.
[22] http://www.wolfram.com/